世界数学



哥德巴赫猜想

辽宁教育出版社

名题欣赏

哥德巴赫猜想 辽……版社

世界数学名题欣赏丛书

哥德巴赫猜想

陈景润 邵品琮 编著



辽宁教育出版社
1987年·沈阳

哥德巴赫猜想

陈景润　邵品琮　编著

辽宁教育出版社出版　辽宁省新华书店发行
(沈阳市南京街6段1里2号)　朝阳新华印刷厂印刷

字数:100,000　开本:787×1092 1/32　印张:6 3/4　插页:4
印数:1—4,254
1987年12月第1版　1987年12月第1次印刷

责任编辑:俞晓群 谭　坚　责任校对:言　覃
封面设计:安今生　插　图:安　迪

统一书号:7371·508　定价:1.45元
ISBN 7-5382-0199-8

内容简介

本书是“世界数学名题欣赏丛书”之一。哥德巴赫猜想是1742年德国数学家哥德巴赫提出的一个数论问题，由于它叙述简明、论证艰深，所以被誉为“数学皇冠上的明珠”。本书在讲解数论基础知识的基础上，详尽地介绍了哥德巴赫猜想的研究历史和成果，内容丰富，观点精当。本书作者曾在哥德巴赫猜想研究中取得卓越成就，书中介绍了他们的数学思想，并展望了猜想的研究方向。

Summary

This book is one of A Series of World Famous Mathematics Appreciation.Goldbach conjecture is a problem of number thery posed by French mathematician Goldbach in 1742. It is reputed as "the pearl in maths crown" for its brief narration and profound proof. This book introduces in detail the history of research in Goldbach conjecture and achievements on the basis of essential knowledge of number theory.The book has substantial content with precise and appropriate views. The author has made remarkable achievements in Goldbach conjecture research. The book introduces their mathematic thoughts and looks forward to the orientation of the conjecture research.

序

自从1742年德国人哥德巴赫(Goldbach)提出了任一不小于6的偶数均可表为两奇素数(prime)和的猜想以来，已经历经了两个半世纪的探索，虽然至今为止，尚未被人证实猜想的正确性，也没有人予以否定，但是围绕这个猜想所作的研究，却积累了相当多的资料与成果，特别是本世纪中近50年来，进展迅速，成绩显著，对于哥德巴赫猜想的研究，达到了非常精深的境界。对于进一步最终研讨哥德巴赫猜想有着极为重要的前沿作用与密切相关的参考价值。

本书作者根据在数学研究工作中的一些经验教训，包括在哥德巴赫猜想的前沿阵地上研究工作的体会，感到在进攻如哥德巴赫猜想这一类世界数学难题的过程中，一是应当了解此类问题的内容与难度，二是应当积累必要的理论基础，三是应当学习已有成果的丰富经验。正因为如此，作者诚恳希望有志青年务必遵照以上三条，力争

在一个扎实的基础上奋勇前进!

哥德巴赫猜想是数论中的一个世界难题。而数论主要是研究自然数的整除性的学问。为此，我们编写了前五章。其中第一、第二两章谈记数方法的由来及自然数与素数的关系，而第三、第四及第五共三章就是讲的整除性。

诚如一开始所说，所谓哥德巴赫猜想是指将偶数表为两奇素数和的问题，那么，素数在自然数中的分布大致如何呢？这是首先应当了解的基本知识，这正是本书第六章的内容。接着我们就在第七章中，详细而通俗地介绍了关于哥德巴赫猜想的研究状态，其中包括了本书作者之一的研究成果的一般介绍。

许多数论问题包括哥德巴赫问题在内，均与数论中的恒等式变化和不定方程的求解等密切相关。在介绍哥德巴赫猜想这一主题成果时，也应当顺便涉及恒等式与不定方程的内容，为此，我们又特地增写了第八、第九两章，并且在第九章末又着重介绍了我们的已故导师华罗庚教授在运用不定方程与恒等式关系来理解哥德巴赫猜想上，一个新的有趣的尝试。

当代数学家们在运用解析数论方法来处理哥德巴赫猜想的研究中，成果的不断更新挺进，往

往与筛法的不断改进有关。本书作者之一（陈景润）对哥德巴赫猜想的最新改进就全仗筛法的运用。因此，我们又特地增添了哥德巴赫猜想与筛法这一章，作为本书最后第十章的内容。

最后，本书作者非常感谢青年数学家张明尧博士在协助本书编写过程中所给予的全力帮助！

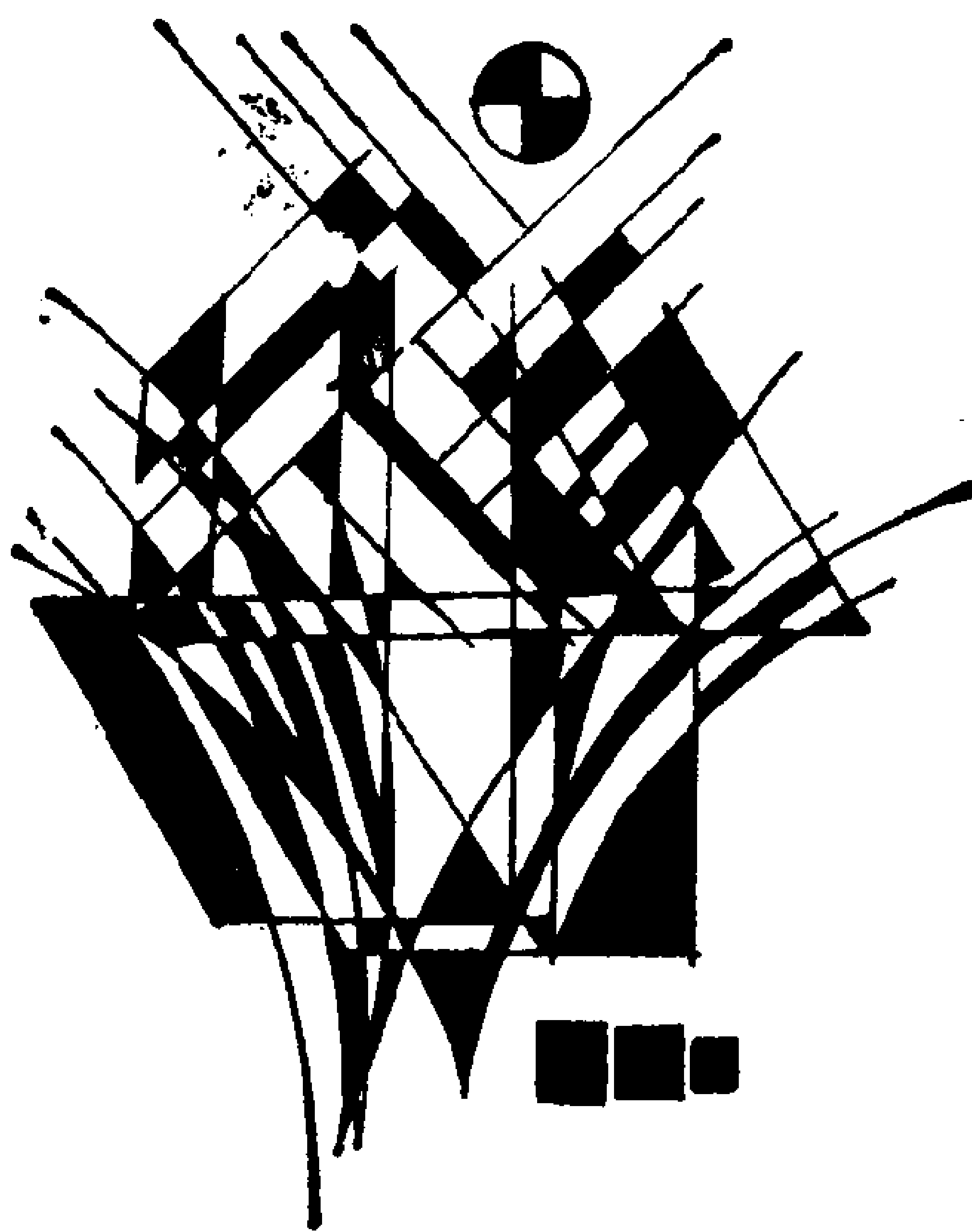
陈景润　邵品琮

1987年元旦，于北京中国科学院数学研究所

目　录

Contents

一 记数的历史



刚刚学会说话的小孩，总在练习“一、二、三、四、…”地数(shǔ)数（shǔ).那么，当初人类是怎样认识数(shǔ)数(shǔ）的呢？原来，最早人们的生产力很低，对数（shǔ）与形的认识与应用也很差，例如渔猎时期，人们打了一只野兔便在系带上打一个结把，绳子上的结多了，也就表明了打的野生动物就多了。起先人们只会数(shǔ)一、二，而三个或三个以上时就数(shǔ)不清了，均称之为“多”吧。这种现象直到现代尚有一些不发达地方还有类似迹象。例如澳大利亚波利尼亚群岛——南太平洋岛屿，法国殖民地，包括土阿莫土群岛、社会群岛等，以及托列斯海峡群岛——在澳洲与新几内亚之间，那里的一些不发达民族的语言里就只有头几个自然数的名称。如只有1和2，3就叫2—1，4叫2—2，5叫

2—2—1，6叫2—2—2，6以上就叫“多”，说成“许多”或“无数”之类的话了。《周易·系辞》中说：“上古结绳而治，后世圣人，易之以书契”.这里“书契”是指在骨头上或竹、木、石片上刻字。《周易·系辞》里的这一句话的意思是说：开始结绳记数（shù），后来才改为用刻画符号在骨头或竹石片上来代替绳，于是产生了文字。所以，人们开始会“记数（shù）”是很早的，它产生在文字出现之前。随着生产力水平的逐渐提高发展，人们对语言文字及记数方式均有了相应的发展与提高。其中历史上对记数（shù）方法的演变与比较过程可举例如下：

（1）汉字：

一　二　三　四　五

（2）甲骨文（殷）：

一　二　三　亖　X

（3）鼎文（周秦金文——镌刻在金属钟鼎器皿上的文字，也叫鼎文）：

一　二　三　亖（X）

（4）《说文解字》（许慎作）里：

一 二 三 亖 X

其中头三个字古今没有变化，它是古算筹或手指的象形。“四”开始有了变化，有如下写法：

这可以在郭沫若先生的《甲骨文字 研 究》 中 见到，后面几个表示是口里呼气读“四”（sì）的样子。

（5）我国古代用算筹记法。大概不会晚于公元前3世纪，甚至可推到战国初期（公元前5世纪）：

纵式：

| ‖ ||| |||| ||||| ⊤ ╥ ╥| ╥||

横式：

一 二 三 ☰ ☰ ⊥ ⊥ ⊥ ⊥

1 2 3 4 5 6 7 8 9

而且会用十进位记数法了，如

⊥⊥=⊥̲̲ 表示6728。

ⅠⅡ Ⅲ 它表示6708,会用空档表零了。

（6）中美洲尤卡坦(Yucatan）半岛（墨西哥东部）的印第安人马雅（Maya）部族，会用20进位制来记数，他们用的记数方法是：

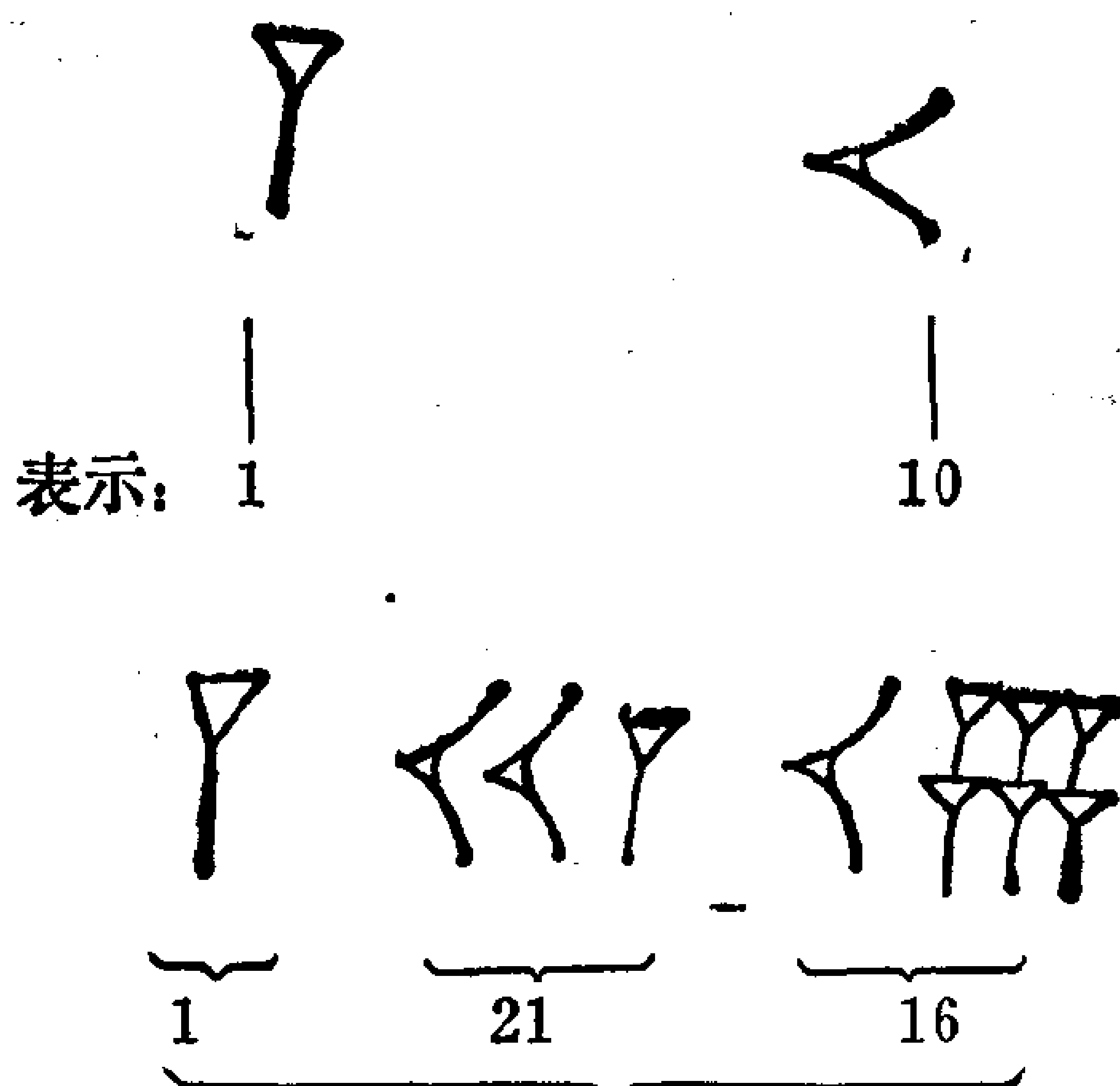
1	5	零（0）
石　子	小　棒	半闭的眼睛（大概是贝壳）

这表示13

这表示有两层构成的数，头一层在下面是17，第二层高一档在上面是8，因为是20进位法，故这个数字是：$8\times 20+17=177$。

（7）巴比伦人会用60进位制，他们的记数

法是：



表示：相当于十进位的4876

这是一个由三位数组成的数。

第三位为16，

第二位为21，

第一位为1。

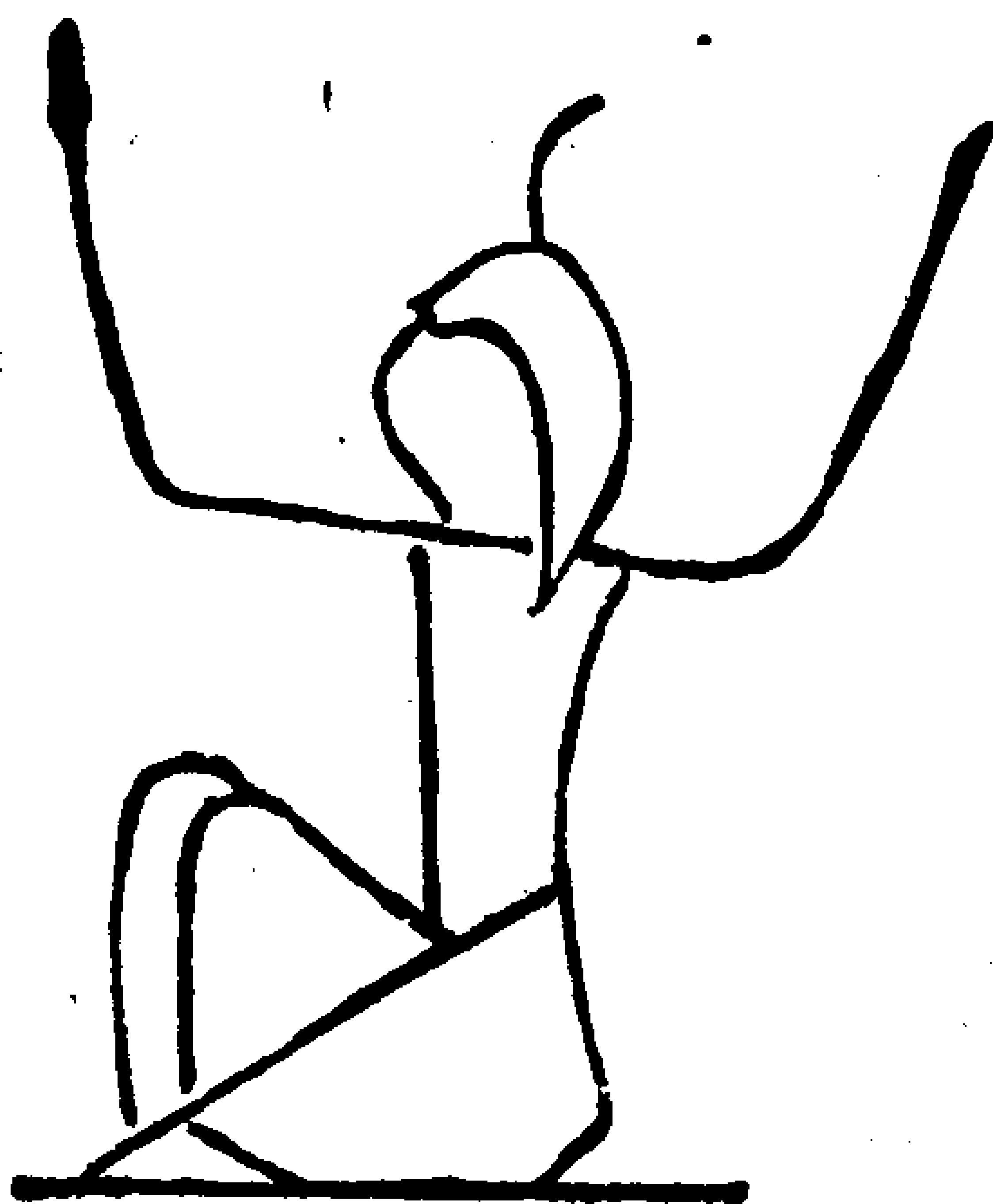
由于是60进位制，故该数为：

$$1\times60^2+21\times60+16=4876.$$

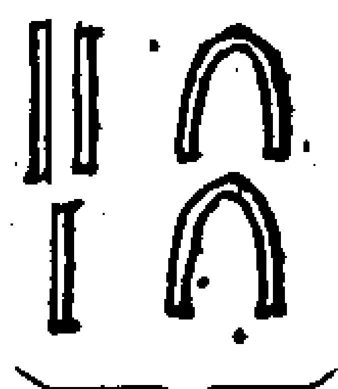
（8）古埃及人很早就会用10进位记数法了，但不会用位值制，例如32与23可用同样的字母在不同位置上安放能表示不同值，这一点他们不懂。他们的记数法是：

表示：1　10　100　1000　10000　100000

杖形　面包形　蛇形　忘忧树形　指着东西的手指形　鸟形



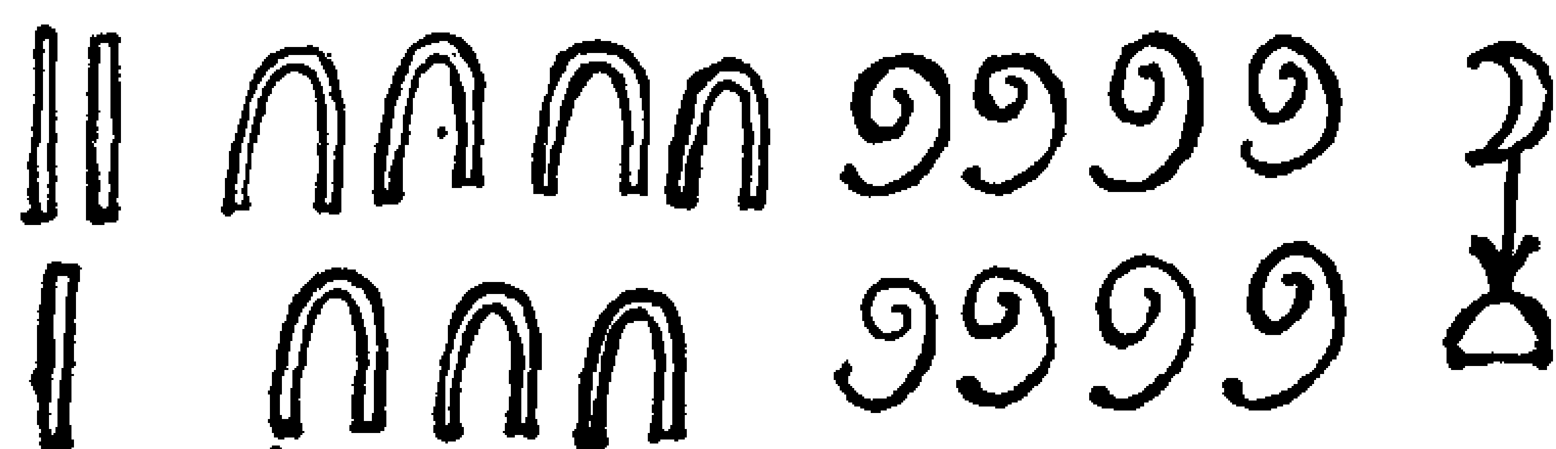
表示：1000000 一百万，人形画成一个好象是受惊的人样子。



表示：23



表示：32



表示：1873（从右往左表高位到个位）

（9）罗马字记数法是：

Ⅰ Ⅱ Ⅲ Ⅳ Ⅴ

表示：1 2 3 4 5

Ⅵ Ⅶ Ⅷ Ⅸ Ⅹ

6 7 8 9 10

其中：

"5"： V 表示一只手四指合并，姆指张开的形状。

"10"： X 表示两只手掌。

"4"： IV 表示 5－1＝4，写在左边的数 1 应当减去之意。

"9"： IX 表示 10－1＝9，而：XI 就表示11了。

（10）印度人用梵文（印度古代文字），大约公元2世纪时，记数法为：

表示：2　3　4　5　6　7　8　9

8世纪以后写成：

表示：1　2　3　4　5　6　7　8　9　0

13世纪在君士坦丁堡（现在的伊斯坦布尔 Istanbul）一个僧人普兰尼达（Maximus Planudes）的书中又改变成：

表示：1　2　3　4　5　6　7　8　9　0

15世纪（1480年）英国的卡克斯敦（William Caxton）出版的书中，数码已接近现代。用：

表示：1　2　3　4　5　6　7　8　9　0

这里应当特别提到的是13、14世纪时印度人用10进制，而由阿拉伯人传播于西方，采用了阿拉伯字母，经若干演变而成了今天的写法，虽然直到16世纪时，巴比伦人还在用60进位制，影响了世界记数法的推广应用.这种情况到16世纪末时，比利时的一位宫廷高级官员名叫斯蒂文（Simon stevinus)的，他还是一位工程师和财政家，当众演示了用十进位制分数进行运算比巴比伦60进位制动算简单得多的效果。这样在实践和科学的基础上被肯定了下来，自16、17世纪后，用阿拉伯字母0，1，2，3，4，5，6，7，8，9为基数的十进位记数法就成为了全世界通用的记数法了.

这里要特别提一下记数法与现代计算机出现的变化关系。在电子计算机出现之前，十进制在所有的数值计算领域内占有至高无上的地位。由于电子计算机运用电路开关系统，而“开”“关取值只有两个，例如0与1，再加上理论地说，进位制中数码信息最经济的是应当用二进位制或三进位制，因此，在运用计算机工作时的记数法就采用了二进位制。当然我们大多数人均是在十进位制运用中成长起来的，但只需要经过不多的简单的努力，就可以象对十进制一样的对二进位制运

用自如的。因此，由于要输入计算机的数，通常是以十进位制给出的，所以需要一架简单的机械把它们变为二进位数，并在末了把答案仍用十进位制来表示，以适应社会上缺少数学训练的人。

二进制数字 0，1 被称为比特，这是 bits 的音译（bits是英文二进制数字BInary digits的缩写）。二进制的基数是 2，十进制的基数为10，例如 $N=1971$ 这个十进制数字，它表示 $1\times10^3+9\times10^2+7\times10+1$。而二进制中，$N$ 的表示可以反复用 2 除得到：

$$1971=985\cdot2+1,\quad 985=492\cdot2+1,$$
$$492=246\cdot2+0,\quad 246=123\cdot2+0,$$
$$123=61\cdot2+1,\quad 61=30\cdot2+1$$
$$30=15\cdot2+0,\quad 15=7\cdot2+1,$$
$$7=3\cdot2+1,\quad 3=1\cdot2+1,$$
$$1=0\cdot2+1.$$

因此 N 在十进制与二进制中的表示为：

$$N=1971_{10}$$
$$=(1,1,1,1,0,1,1,0,0,1,1)_2.$$

由于二进制中数的表示较长，计算机语言常常利用八进制（基数为 8），这只是二进制的一种简单变形，它按二进制中表示的数字三位数一组分组获得。基数为 $8=2^3$，其系数是如下八个数：

$$0=000,\ 1=001,\ 2=010,$$
$$3=011,\ 4=100,\ 5=101,$$
$$6=110,\ 7=111.$$

用这种方式，上述N为

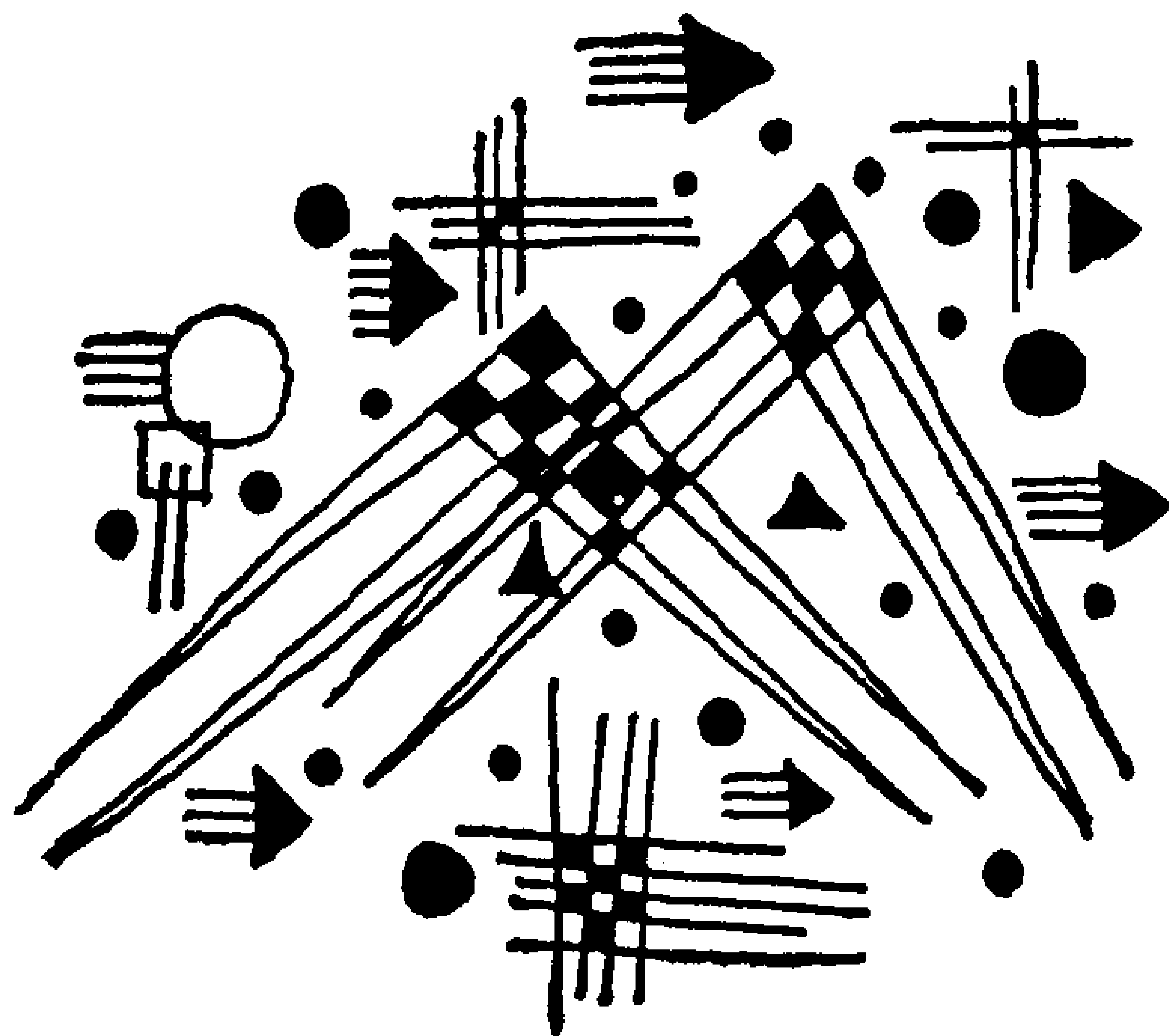
$$N=1971_{10}=011,110,110,011$$
$$=(3;6;\ 6;3)_8.$$

在计算机中，还有另外一些数的表示法是很有用的。这些，关于记数法在计算机语言中的特殊性我们就大致介绍到这里。

用十进位记数法来数(shǔ)数(shù)，可以由1，2，3，4，…地数下去到10，然后11，12，13，…又到20，再21，22，…，如此下去。一个小孩开始练数一百，往往很费劲数到了一百，再自我得意一下，多数几个：101，102，103等等，就算是很不错的孩子了。但是，即使是很有经验的成人到底又能数到那一位数字呢？原来，如此数(shǔ)数(shù)是数不完的，是无穷多的。这件事，有个数学家名叫菲耶诺（Peano)的，他指出这种数(shǔ)数(shù)的原则：从1开始，之后任何数a(包括1在内)总用它本身的数(shù)加1（叫后继数)作为它相邻的后一个数(shù)，并记为a^+（那么有$a^+=a+1$），例如1，$1^+=1+1=2$，$2^+=2+1=3$…，如此下去，由1开始

及$a^+=a+1$的办法，总是由 a 后继a^+而数(shǔ)下去而构成的所有 数(shù)，称为自然数集（这里说明一下，一些逻辑学家与代数学家，有时喜欢由 0 开始，按后继数递增来数(shǔ)数(shù)而演成的全体数(shù)称为自然数集，即指{0，1， 2，3，…}它包括了"0"也是一个自然数。但由于我们后面要讲到的数论知识里，总要讨论到用自然数当除数的问题，为了常可略去除数中自然数非零的声明，我们所定义的自然数集就不包括"0"，因此，今后一切自然数{1，2，3，…}必然非零）．上述这个数(shǔ)数(shù)原则，在数学史上称为非耶诺公理。那么，根据非耶诺公理知道，全体自然数（即自然数集 $N=\{1,2,3,\cdots\}$）的"个数(shù)"是数(shǔ)不完的，即无穷多的。

二 自然数与素数



既然自然数是无穷的，将全体自然数添上一个零以及它的全体负数，放在一起称为整数集。那么在整数集中取出任意两个整数 a 与 b 来，作加法，减法，乘法，其结果仍是整数，然而若作除法的话就不一定除得出商为整数了。故而四则运算对整数来说，最应当注意的是除法。对待自然数的除法来说，当除数非零时研究除得尽还是除不尽的学问便是“数论”这一门数学分支的中心课题。现在如果任意拿出两个自然数 a 与 b 来，作除法。例如令 a 除以 b，而设$b>0$，我们规定其商取为整数，当然就有可能产生余数，假若恰好除尽（余数为零时），其商为 q，可写为 $a\div b=q$，或$a=b\cdot q$，此时就说 a 是被 b 整除，记成$b|a$，称 b 为 a 的因子，而 a 称为 b 的倍数，例如$a=24$，$b=4$，有$q=6$，那么 4 就是 24 的因

数，而24是4的倍数，假若商为整数而仍有余数非零的话，就说是除不尽的，记成$b\nmid a$，例如$a=24$，$b=5$就是一例（$5\nmid 24$）。

假若$a=1$，当然只有$b=1$是它唯一的因数，故我们称自然数1为“单位数”。当取自然数$a\geqslant 2$时，b取1和a两个数是其当然因数，有的数除了1和它本身这两个当然因数之外，并无其它因数时，称为素数，例如2,3,5,7,11,13,17,19,23，…等等。素数有时记为$p,p',p_1,p_2,\cdots$等等，有的自然数除了两个当然因数以外，如果尚有其它的因数者（例如$a=24$时，可取$b=1,24$，以及2,3,4,6,12为其因数），就称为合数。

现在从大于或等于2的自然数中，任选一个，例如是n，$n\geqslant 2$，那么有两种可能：要么是素数，要么是合数。如果它是素数，就改写为p；如果它并非素数，那么除了1和它本身n以外，尚有其它因数，例如有$n_1|n$而$2\leqslant n_1\leqslant n-1$。因而是写$n=n_1\cdot n_2$其中商数$n_2=n\div n_1$也是一个整数，它也是$n$的一个因数。并且易见有$2\leqslant n_2=\dfrac{n}{n_1}\leqslant\dfrac{n}{2}$，从而又得$2\leqslant n_1=\dfrac{n}{n_2}\leqslant\dfrac{n}{2}$，由此可见，只要$d|n$，且$d\neq 1$及$n$，则总有$2\leqslant d\leqslant\dfrac{n}{2}$。如果式$n=n_1\cdot n_2$中的$n_1$

是素数因数，就改写为p_1，若n_2也是素因数，也即改写为p_2，此时得$n=p_1p_2$是两个素数的连乘积；假若n_1，n_2两个因数中有一个为合数，例如n_2是合数，则同样道理就有两个整数m_1，m_2使得$n_2=m_1\cdot m_2$其中仍有

$$2\leqslant m_1\leqslant\frac{n_2}{2},\quad 2\leqslant m_2\leqslant\frac{n_2}{2}$$

如果m_1，m_2均为素数，则改写为p_2，p_3，于是有$n=n_1n_2=p_1n_2=p_1p_2p_3$为三个素数的连乘积；假若$m_1$，$m_2$之中又有合数．或者当初$n_1$本身也是合数时，则再作类似的分解处理．如此下去，直到全出现素数改写为若干个p的连乘积为止．请注意，这种分解的步骤是不可能无穷尽地进行的，因为每分解一次，因数数值本身就要至少缩小一半．每次必须保证分出整数因子，因而最多有限次终止，例如c次，则易见应有$2^c\leqslant n$，或$c\leqslant\log_2 n$，这就是说，任一正整数$n\geqslant2$，总可分解成若干个（例如s个）素数的连乘积的：

$$n=q_1\cdot q_2\cdots q_s$$

其中$q_1, q_2, \cdots, q_s$为素数，这就是初等数论中，最基本的素数分解定理，如果我们将这些素数由左到右、从小到大作重新排列，并且将其中相同的素数个数记在相应素数的指数位置上，则就有

形如

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

的分解式，其中素数 $p_1<p_2<\cdots<p_k$，而整数 $\alpha_1\geqslant 1$，$\alpha_2\geqslant 1$，…，$\alpha_k\geqslant 1$，而且这种表示法是唯一的，这就是初等数论中最著名的标准唯一分解定理。

当然，关于素数分解的标准唯一性定理的证明，我们打算放在后面来予以阐明。

既然任意一个自然数$n\geqslant 2$，都可由素数或几个素数的连乘积来表示，自然就问：在整个自然数中素数的个数总共是多少呢？早在二千年前，古代数学家欧几里得(Euclid)就曾指出了素数的个数是无穷的，而且还给出了一个不朽的证明：用反证法，如果素数的个数是有限的，例如设为m个，记成 $p_1,p_2,\cdots,p_m$，不妨认为这m个素数为 $p_1<p_2<\cdots<p_m$。以下我们将引出矛盾。事实上，我们可考虑一数

$$M=p_1p_2\cdots p_m+1$$

由于素数一共m个，而p_m已是最大素数。今$M>p_m$，故而M决非素数。因而它是一个合数。利用素数分解定理，就有素因数 $q_1,q_2,\cdots,q_s$使$M=q_1q_2\cdots q_s$，其中 $s\geqslant 2$，注意因数 $q_1|M$，q_1又必为 $p_1,p_2,\cdots,p_m$中的一个，例如 $q_1=p_i(1\leqslant i\leqslant m)$，于是可改写$M=p_iQ$，其中$Q=q_2\cdots q_s$仍为整数，

七

②

因而

$$p_iQ=M=p_1\cdots p_{i-1}p_ip_{i+1}\cdots+1$$

再记 $P=p_1\cdots p_{i-1}p_{i+1}\cdots p_m$ 也是一个整数，于是由上式，得

$$p_i(Q-P)=1$$

若$Q=P$则左端为 0，右端为 1，矛盾．若$Q\neq P$，则有

$$1=p_i(Q-P)=|p_i(Q-P)|$$
$$=p_i|Q-P|\geqslant p_i\cdot 1=p_i$$

矛盾．从而知素数个数是有限个的假设是不对的，因此素数个数的无穷性证毕．

现在我们可以来证明素数分解的标准唯一性定理（即算术基本定理）了，为此，我们需要先用到一个重要的引理，然后来证实我们的结论，并顺带举一点应用上的例子．

引理2.1 如果 p 是素数，而且 $p|ab$，则必有$p|a$或$p|b$．

证明 可以不妨假定a,b都是自然数，采用反证法，若引理不成立，即若 $p|ab$，而有 $p\nmid a$ 及 $p\nmid b$，将引出矛盾，事实上，由反证假设，那么一定有一个最小的素数p_0使引理不成立，对于这个素数 p_0 又有最小的 a_0b_0 使引理不成立者．即

$p_0|a_0b_0$，而$p_0\nmid a_0$，$p_0\nmid b_0$且*

$$a_0b_0=\min\{ab|\ p_0|ab,\ p_0\nmid a,\ p_0\nmid b\}$$

首先我们来指出必有 $a_0<p_0$，这可用反证法，由$a_0\neq p_0$，故有$a_0>p_0$。所以用p_0除a_0（由$p_0\nmid a_0$）得余数a_1必在 0 与p_0之间：

$$a_0=kp_0+a_1,\ 0<a_1<p_0$$

因此

$$a_0b_0=(kp_0+a_1)b_0=kb_0p_0+a_1b_0$$

由$p_0|a_0b_0$，$p_0|kbp_0$得$p_0|(a_0b_0-kb_0p_0)$即$p_0|a_1b_0$，然而$p_0\nmid a_1$，$p_0\nmid b_0$，从而应当有$a_0b_0<a_1b_0$（按"最小"性定义）即$a_0<a_1$，这与$a_1<p_0<a_0$相矛盾。同理，必有$b_0<p_0$。因此$a_0b_0<p_0^2$。

由于$p_0|a_0b_0$，所以写 $a_0b_0=lp_0$，显然$l\neq 1$，故$l\geqslant 2$，另方面由$a_0b_0<p_0^2$知$l<p_0$。再根据已有的素数分解定理，数 l 可写成若干素数的连乘积，记

$$q_0=\min\{q|q素数,\ q|l\}$$

也就是选 l 的素因数中最小的一个记为 q_0，由$l|a_0b_0$，故 $q_0|a_0b_0$，因为 $q_0\leqslant l<p_0$。由 p_0 为不满足引理的最小素数这一假定知素数$q_0|a_0b_0$，则必有$q_0|a_0$或$q_0|b_0$至少有一个成立，不妨设$q_0|a_0$，

* 记号$\min\{s|A\}$表示：具有性质A的一切 s 中取最小的一个。

记$a_0=a'q_0$，由于$q_0|l$故记$l=tq_0$，代入到 $a_0b_0=lp_0$有

$$a'q_0b_0=tq_0p_0$$

因而$a'b_0=tp_0$，即有$p_0|a'b_0$，且 $p_0\nmid a'$，$p_0\nmid b_0$。今$a'b_0<a_0b_0$，这与 a_0b_0 的"最小"性假设相矛盾。因此我们的这个基本引理证毕。

当然，作为上述基本引理的推广，还可以有如下结论：若素数 $p|a_1a_2\cdots a_m$ 则至少存在一数 $a_i(1\leqslant i\leqslant m)$使得$p|a_i$。

设$n\geqslant 2$，那么它可表成若干素数的连乘积，例如有素数$q_1,q_2,\cdots,q_s$使

$$n=q_1q_2\cdots q_s,\ (s\geqslant 1)$$

如果重新排序，不妨假设 $q_1\leqslant q_2\leqslant\cdots\leqslant q_s$，并且将相同的素数累记到这素数的幂次方上去，则上述分解定理可以改叙为：大于1的自然数n，总可以找到素数因数 $p_1<p_2<\cdots<p_k$，使

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \qquad (*)$$

其中$\alpha_1\geqslant 1,\alpha_2\geqslant 1,\cdots,\alpha_k\geqslant 1$也为正整数。

上面这个式子（*）称为n($\geqslant 2$时)的标准分解式。

那么，我们就有了

定理2.1（算术基本定理） 对于任意自然数$n\geqslant 2$而言，总可以找到素数$p_1,p_2,\cdots,p_k$，及整

数$\alpha_1, \alpha_2, \cdots, \alpha_k$满足$p_1 < p_2 < \cdots < p_k$及$\alpha_1 \geqslant 1, \alpha_2 \geqslant 1, \cdots, \alpha_k \geqslant 1$，使得（*）成立，且这种表示是唯一的。

证明 对于$n \geqslant 2$而言，素数$p_1, p_2, \cdots, p_k$及整数$\alpha_1, \alpha_2, \cdots, \alpha_k$满足$p_1 < p_2 < \cdots < p_k$及$\alpha_1 \geqslant 1, \alpha_2 \geqslant 1, \cdots, \alpha_k \geqslant 1$，使得（*）成立的存在性是由分解表定理及上述解释保证了的。今只须证明它示法的唯一性。实际上，假定n有两种标准分解式

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l} \quad (*)'$$

其中$p_i, \alpha_i (i = 1, 2, \cdots, k)$满足（*）的叙述条件，而素数$q_j$，整数$\beta_j (j = 1, 2, \cdots, l)$满足$q_1 < q_2 < \cdots < q_l$，$\beta_1 \geqslant 1, \beta_2 \geqslant 1, \cdots, \beta_l \geqslant 1$。由基本引理及其推广形式，任何素数$p_i$必定为$q_1, q_2, \cdots q_l$中的一个；任何$q_j$也必定为$p_1, p_2, \cdots, p_k$中的一个。所以必有$k = l$，再由于顺序关系

$$p_1 < p_2 < \cdots < p_k \text{及} q_1 < q_2 < \cdots < q_k$$

所以必有

$$p_i = q_i (i = 1, 2, \cdots, k)$$

下面我们将指出有$\alpha_i = \beta_i (i = 1, 2, \cdots, k)$。证明可用如下方法：若有一个$\alpha_i \neq \beta_i (1 \leqslant i \leqslant k)$，将引出矛盾如下：若$\alpha_i > \beta_i$，则在（*）式中双方约去$p_i^{\beta_i}$，有

$$p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}p_i^{\alpha_i-\beta_i}p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k}$$
$$=p_1^{\beta_1}\cdots p_{i-1}^{\beta_{i-1}}p_{i+1}^{\beta_{i+1}}\cdots p_k^{\beta_k}$$

其中$\alpha_i-\beta_i\geqslant1$，那么$\beta_i$便是$p_1^{\beta_1}\cdots p_{i-1}^{\beta_{i-1}}p_{i+1}^{\beta_{i+1}}\cdots p_k^{\beta_k}$的因数，由基本引理及其推广形式知$p_i$必为上列右端中的一个素因数，即有$p_j$，$j\neq i$使$p_j=p_i$这与$p_1,p_2,\cdots,p_k$为相异素数矛盾。同样，若$\alpha_i<\beta_i$也可以获得类似推理引出矛盾。因此，只有$\alpha_i=\beta_i(i=1,2,\cdots,k)$，这就证实了我们的自然数$n\geqslant2$对于素数分解式的标准形式的唯一性定理。这个定理，不少书本上称它为算术基本定理。

例如证明$\sqrt{2}$为无理数（非有理数），这已是众所周知的了。那里也是用的整除性，紧紧抓住2这个偶数的素数，以及单数的平方仍为单数，平方若为偶数的数必为偶数等等的性质来证明的。

今，再用分解唯一性的定理来予以证明如下：

"$\sqrt{2}$"是平方为2的一个正数，所谓有理数是指形如$\frac{Q}{P}$的数，其中P,Q均为整数，且$P\neq0$。要证$\sqrt{2}$为无理数，采用反证法，设它为有理数（因而为正有理数）$\frac{Q}{P}$，其中$P>0$，$Q>0$，均为自然数，以下将引出矛盾：首先要指出必有$P\geqslant2$，$Q\geqslant2$。因为否则（例如$P=1$时）显然矛

盾（例如当$P=1$时，有$\sqrt{2}=Q$，两边平方$2=Q^2$，显然$Q\geqslant2(Q\neq1)$，Q分解成标准形式$q_1^{\beta_1}\cdots q_l^{\beta_l}$，有$2=q_1^{2\beta_1}\cdots q_l^{2\beta_l}$右方为素数的$\geqslant2$次方幂，这与2这个素数只有唯一标准形式$2^1$相矛盾）。此时，按素数分解标准唯一性定理，可写$P$与$Q$的标准分解式为

$$P=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$
$$Q=q_1^{\beta_1}\cdots q_l^{\beta_l}$$

据$\sqrt{2}=\frac{Q}{P}$，有 $2=\frac{Q^2}{P^2}$，即$Q^2=2P^2$记它为n，

则有

$$n=2^1p_1^{2\alpha_1}\cdots p_k^{2\alpha_k}=q_1^{2\beta_1}\cdots q_l^{2\beta_l}$$

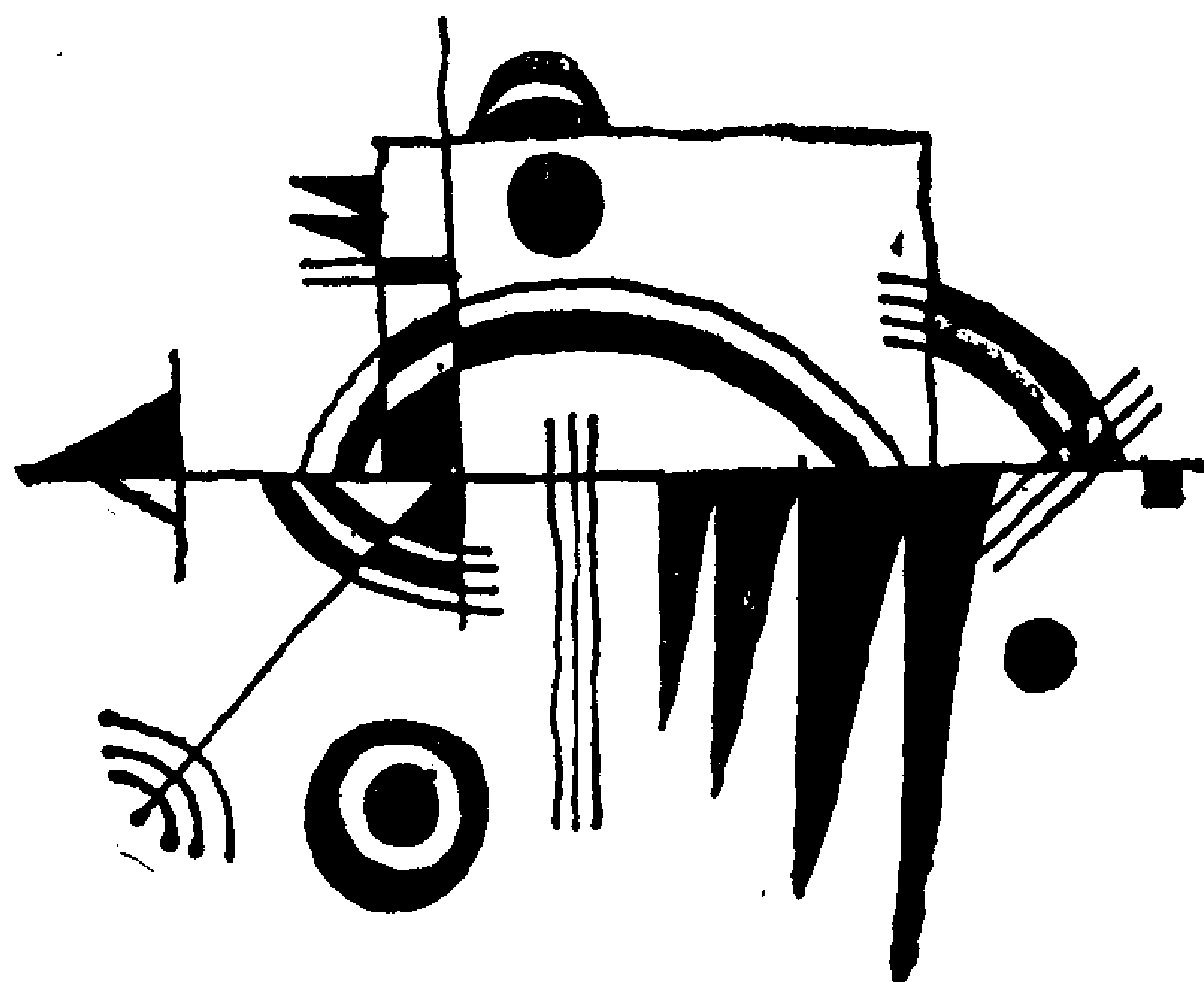
请注意，同一个n，标准分解式中既有素数2的单数次方幂，又是一切因数$q_1,\cdots,q_l$的双数次方幂，这与分解的标准唯一性定理中的“唯一性”结论相矛盾。从而$\sqrt{2}$非有理数得证。

再如可证$\log_{10}2$为非有理数（无理数）：反证法，设$\log_{10}2=\frac{Q}{P}$为一有理数，当然它是正有理数，$P\geqslant1$，$Q\geqslant1$，于是有

$$2=10^{\frac{Q}{P}}\Rightarrow2^P=10^Q\Rightarrow2^P=2^Q5^Q$$

这又与数$n=2^P=2^Q\cdot5^Q$的标准分解的唯一性相矛盾。故$\log_{10}2$决非有理数，必为无理数。

三 自然数的除法



“数”与“量”是我们数学研究的对象。最早，数(shù)起源于数(shǔ)如一，二，三，四，五，…地数(shǔ)下去.量(liàng)起源于量(liáng)如一米，二米，三米，四米，五米，…地量(liáng)下去。凡是量(liàng)总可以用一个单位量(liàng)来量(liáng)，于是就要数(shǔ)，便数(shǔ)出了数(shù).所以“数”与“量”是紧密联系的，有了这个“数”(shù)就反映了那个被量(liáng)的“量”(liàng)。因此，要想反映一个长度的大小，就得用另一个长度去量(liáng)，经过数(shǔ)数(shù)而得其量(liàng)。当然，量(liáng)长度时，往往总是习惯地用短的去量(liáng)长的。

长的叫 l，短的叫 m，如果正好量了几下，例如量了 k 次正好量尽的话，就说 l 是 m 的 k 倍，记为 $l=km$；否则，量到某一个步骤例如 k

次后，尚有余，余下一段记为r，而再量一次（即量到$k+1$次时）就不够了，说明 $0<r<m$，这时可写 $l=km+r(0<r<m)$。总之，任意两个实数 l 与m（其中$m>0$），总存在一个正整数k，使得

$$l=km+r,\ (0\leqslant r<m)$$

这件事，称为阿基米德（Archimede）原理。如果l，m为两个自然数的话，这个原理称为带余除法，有正规的定理为：

定理3.1（带余除法） 设 a，b 是两个整数，其中$b>0$，则存在两个整数 q 及 r，使得

$$a=bq+r,\ 0\leqslant r<b \qquad (3.1)$$

而且 q 及 r 是唯一的。

证明 作整数序列

$$\cdots,-3b,-2b,-b,0,b,2b,3b,\cdots$$

则 a 必在上述序列的某两项之间（阿基米德原理），即存在一个整数 q 使得

$$qb\leqslant a<(q+1)b,$$

令$a-bq=r$，那么有 $0\leqslant r<b$。为证 q，r 的唯一性，今设 q'，r' 是满足（3.1）的另一组整数，那么有

$$a=bq+r=bq'+r'$$

或

$$b(q-q')=r'-r$$

因此

$$|r-r'|=b|q-q'|\Longrightarrow b\,|\,|r-r'|$$

若$r\neq r'$则$|r-r'|\neq 0$，由$0\leqslant r<b$及$0\leqslant r'<b$知$0<|r-r'|<b$，这与$|r-r'|$为b的倍数相矛盾．故只有$r=r'$。由$b>0$知必有$q=q'$。这就证得了（3.1）中的q，r是唯一的。

由这个带余除法定理3.1，我们还可以把带余除法用另外的形式来表示的．例如有：

定理3.2 若a，b是任意二整数，且$b\neq 0$，则存在两个整数s，t使得

$$a=bs+t,\quad |t|\leqslant\frac{|b|}{2} \tag{3.2}$$

并且当b为单数（奇数）时，s，t是唯一的。

当b为双数（偶数）时，就不一定了。例如$a=26$，$b=4$，可以有两种表达式：

$$26=6\times 4+2$$

$$26=7\times 4-2$$

其中s，t可取：$s=6$，$t=2$或$s=7$，$t=-2$，均有$|t|=\dfrac{|b|}{2}$。

下面，作为带余除法的应用，我们在因数判别法中略举几例．

一个正整数A，如果它在十进位表示中为

$a_n a_{n-1} \cdots a_2 a_1 a_0$共$n+1$位数，其中每一位为

$$0 \leqslant a_i \leqslant 9, \quad (i=0,1,2,\cdots,n)$$

实际A的数字大小为

$$A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0$$

因为10以及10的任何幂均能被2所整除，故而若a_0能被2整除（双数），则A能被2整除，反之也对，故有*

$$2 \mid A \rightleftarrows 2 \mid a_0$$

也即只需看个位数是否偶数，就可判断原数A是否偶数，这是众所周知的常识。同理还有

$$5 \mid A \rightleftarrows 5 \mid a_0$$

也即只需看个位数是否为0或5，就可判断原数A是否为5的倍数了。

如何判断A是否为3的倍数呢？首先看：有

$$10 = 3 \times 3 + 1, \quad 10^2 = 3 \times 33 + 1, \quad \cdots,$$

$$10^n = 3T_n + 1.$$

也即任何一个10的幂方，如10^k，总可写成被3除余1的形式：

$$10^k = 3 \times T_k + 1$$

其中T_k为一个正整数。故而

---

* 记号"$\rightleftarrows$"表示充分且必要的条件，例如"甲$\rightleftarrows$乙"表示：由甲可推出乙，而且反之，由乙可推出甲。

$$a_k \times 10^k = 3 \times T_k \times a_k + a_k = 3T_k^1 + a_k$$

因此有：

$$A = \sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} (3T_k^1 + a_k)$$

$$= 3\sum_{k=0}^{n} T_k^1 + \sum_{k=0}^{n} a_k = 3T + \sum_{k=0}^{n} a_k$$

其中

$$T = \sum_{k=0}^{n} T_k^1 = \sum_{k=0}^{n} a_k T_k$$

仍为一个正整数。这样一来，就有

$$3 \mid A \rightleftarrows 3 \mid \sum_{k=0}^{n} a_k$$

也就是说，一个$n+1$位数$A = a_n a_{n-1} \cdots a_2 a_1 a_0$是否为 3 的倍数，只要看其各位数之和是否为 3 的倍数就可完全确定。使如$A = 5874192$，由 $5+8+7+4+1+9+2=36$知A为 3 的倍数。

如何判断A是否为11的倍数呢？仍看10的各幂方数，有

$$10 = 11 - 1,$$

$$10^2 = (11-1)^2 = 11 \times T_2 + 1,$$

$$10^3 = (11-1)^3 = 11 \times T_3 - 1, \cdots$$

$$10^k = (11-1)^k = 11 \times T_k + (-1)^k.$$

故而 10^k 总可以写成被 11 除余数为± 1 的形式

$(-1)^k$. 因此有

$$
\begin{aligned}
A &= \sum_{k=0}^{n} a_k 10^k \\
&= \sum_{k=0}^{n} (11 \times T_k + (-1)^k) a_k \\
&= 11 \sum_{k=0}^{n} a_k T_k + \sum_{k=0}^{n} (-1)^k a_k \\
&= 11T + \sum_{k=0}^{n} (-1)^k a_k
\end{aligned}
$$

其中 $T = \sum_{k=0}^{n} a_k T_k$ 为一整数，故而

$$11 \mid A \Longleftrightarrow 11 \mid \sum_{k=0}^{n} (-1)^k a_k$$

将 $a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$ 写成两部分：一为正项和，记为S^+，另一项为负项和，记为S^-，即

$$S^+ = a_0 + a_2 + \cdots, \quad S^- = a_1 + a_3 + \cdots$$

那么

$$\sum_{k=0}^{n} (-1)^k a_k = S^+ - S^-$$

于是得

$$11 \mid A \Longleftrightarrow 11 \mid S^+ - S^-$$

也即就看这个A的各位数中，交错位数间隔相加的两个总和，其差是否为11的倍数即可判定A为11的倍数与否。例如$A = 75312289$非11的倍数，而$11 \mid 137093$。

大家知道，含有未知数的等式称为方程式，或简称方程。如果变数个数有二个或二个以上，且要求解答为整数的方程，通常称为不定方程。关于不定方程方面的一些知识，我们在第四章及第八章中将予以阐明。今作为可除性应用，来试举一例，讨论一个如下形式的不定方程：

$$x^2-3y^n=-1(n\geqslant1) \tag{3.3}$$

我们要证明它没有任何整数解。可用反证法，设有整数解（x_0,y_0）满足上述方程，将引出矛盾。实际上，既然有恒等式

$$x_0^2\equiv3y^n{}_0-1(n\geqslant1) \tag{3.4}$$

那么，用x_0被3除，余数记作r_0，有

$$x_0=3t_0+r_0,\ (0\leqslant r_0\leqslant2)$$

平方之，有

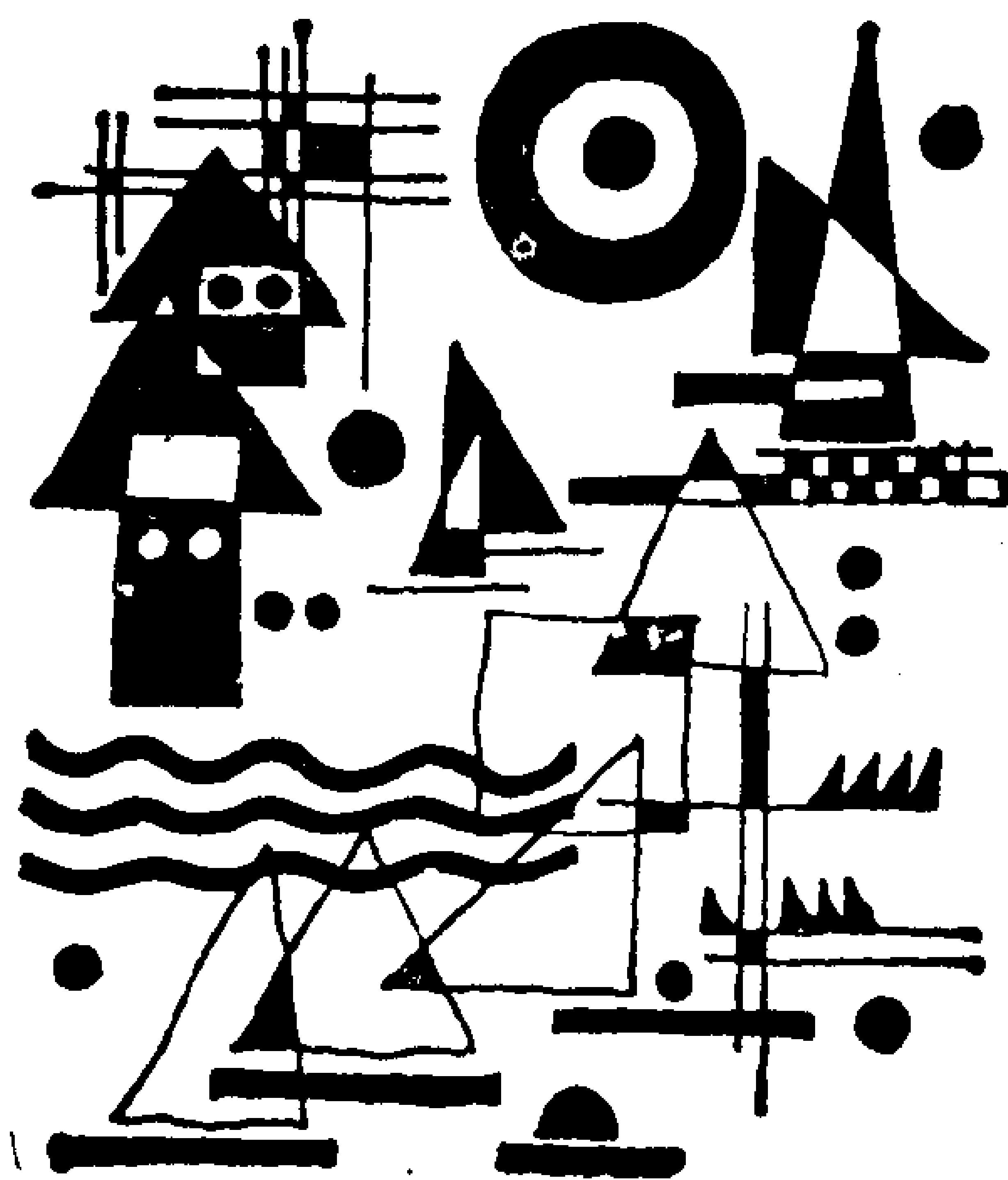
$$x_0^2=(3t_0+r_0)^2=3t_1+r_1 \tag{3.5}$$

其中$r_1=0$或1。比较（3.4）与（3.5），便得

$$r_1+1=3\cdot(y^n{}_0-t_1) \tag{3.6}$$

此处（3.6）的左端大于0而小于或等于2。它不可能为3的倍数，故与（3.6）的右端矛盾。因此原方程（3.3）无整数解得证。

四 长 除 法



在介绍数论基本知识的过程中，"公因数"的概念是非常重要的。

已知两不同时为 0 的整数a，b，若有一整数d，既是a的因数，又是b的因数，则称d为a与b的公因数。在a与b的一切公因数中最大的一个d^*称为是a与b的最大公因数。用数学上的符号记法来说，最大公因数的定义为：

$$d^* = \max\{d|\ \ d|a \& d|b\} \qquad (4.1)$$

记成$d^* = (a,b)$。这里(a,b)表示a与b的最大公因数。

（记号$A \& B$ 表示：既有A同时又有B）

定理4.1 设a和b是不同时为 0 的整数，而且$d_0 = ax_0 + by_0$是形式$ax + by$（x,y是整数）的数中最小的正数。则$d_0 = (a,b)$。

证明 注意

$$d_0=\min\{d|d=ax+by,\ d>0\}\qquad(4.2)$$

要证 $d_0=(a,b)$。先证 d_0 为 a 与 b 的公因数. 为此，先证$d_0|a$，用反证法，设 $d_0\nmid a$，由 $d_0>0$，有$a=d_0a_0+r$，$0<r<d_0$。

于是

$$r=a-d_0a_0=a-(ax_0+by_0)a_0$$
$$=a(1-x_0a_0)+b(-y_0a_0)$$

这说明 r 为形如$ax+by$的数，且$r>0$，而今$r<d_0$，这与d_0 为最小的形如 $ax+by$ 的正数相矛盾，故而$d_0|a$。同理$d_0|b$.因此 d_0为 a 与 b 的公因数，今记 a 与 b 的任一公因数为d，并记

$$a=da',\ b=db'$$

则有

$$d_0=ax_0+by_0=a'dx_0+b'dy_0$$
$$=d(a'x+b'y_0)$$

于是

$$d|d_0\Longrightarrow d\leqslant d_0,\ (\forall d)$$

这说明d_0是最大的一个公因数。故$d_0=(a,b)$。□

从上面的证明过程，可以引出如下最大公因数的另一种定义：

定理4.2 设 a 和 b 是不同时为 0 的整数，如果有一个整数d_*，它具有下列两个性质：

1）d_*为 a 与 b 的公因数；

2）一切 a 与 b 的公因数 d 均能整除d_*，则 $d_* = (a,b)$。且反之也对。

证明 注意d_*满足

1）$d_* | a \& d_* | b$，

2）若$d | a \& d | b \Longrightarrow d | d_*$。　　　　(4.3)

由 1）知，d_*为 a 与 b 公因数，由 2）知必有 $d \leqslant d_*$故d_*为最大一个公因数，因此 $d_* = (a,b)$，如今要证的是若$d_* = (a, b)$。要论证d_*必满足上述 1）与 2）.首先满足 1）是当然的。现记 a 与 b 的任一公因数为 d，并记 $a = da'$，$b = db'$，那么由定理4.1知$d^* = d_0$，有两整数 x_0，y_0 使得 $d_0 = ax_0 + by_0$，于是

$$d^* = ax_0 + by_0 = a'dx_0 + b'dy_0$$
$$= d(a'x_0 + b'y_0)$$

这说明必有$d | d^*$。　□

推广一下，已知 s 个不同时为 0 的整数 a_1，a_2，…，a_s，若有一整数 d，它是一切 a_i 的因数 $(i = 1,2,\cdots,s)$，则 d 称为a_1，a_2，…，a_s 的公因数，在a_1，a_2，…a_s 的一切公因数中最大的一个d^*称为是a_1，a_2，…，a_s的最大公因数。即最大公因数的定义为：

$$d^* = \max\{d | \quad d | a_i,\ i = 1,2,\cdots,s\}$$

(4.4) 记成$d^* = (a_1, a_2, \cdots, a_s)$，

相应地有

定理4.3 设a_1，a_2，…，a_s是不同时为0的整数，而且$d_0=a_1x_1^*+a_2x_2^*+\cdots+a_sx_s^*$是形式$a_1x_1+a_2x_2+\cdots+a_sx_s$（$x_1$，$x_2$，…，$x_s$是整数）的数中最小的正数，则$d_0=(a_1, a_2, \cdots, a_s)$。

定理4.4 设a_1，a_2，…，a_s是不同时为0的整数。如果有一个整数d_*它具有下列两个性质：

1）d_*为a_1，a_2，…，a_s的公因数；

2）一切a_1，a_2，…，a_s的公因数d均能整除d_*。

则 $d_*=(a_1, a_2, \cdots, a_s)$，且反之也对。

这两个定理的证明时，也即在证明这三种定义的等价性时，要注意到第一种定义$d^*=(a_1, a_2, \cdots a_s)$满足（4.4）；第二种定义$d_0$，满足（4.5）式：

$$d_0=\min\{d \mid d=a_1x_1+a_2x_2+\cdots+a_sx_s,\ d>0\} \qquad (4.5)$$

第三种定义d_*满足条件

1）$d_* \mid a_i \quad i=1, 2, \cdots, s$。

2）若$d \mid a_i$，$i=1, 2, \cdots, s$。$\Longrightarrow d \mid d_*$

(4.6)

然后完全仿照上述$s=2$时的情形叙述即成，此处不再赘述。

顺便提一下，如果两个复合数a与b的标准

分解式中，公共素因数为 p_1，p_2，…，p_k，其余素因数相等。则 a 与 b 可改写一下为

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}f_1^{s_1}\cdots f_\lambda^{s_\lambda}$$

$$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}g_1^{t_1}\cdots g_\mu^{t_\mu}$$

$\alpha_1\geqslant 1$，…，$\alpha_k>1$；$s_1\geqslant 1$，…，$s_\lambda\geqslant 1$；$t_1\geqslant 1$，…，$t_\mu\geqslant 1$；而f_1，…，f_λ；g_1，…，g_μ 均为相异素数，那么就有最大公因数为：

$$(a,b)=p_1^{c_1}p_2^{c_2}\cdots d_k^{c_k}$$

其中

$$c_i=\min(\alpha_i,\beta_i),\ i=1,\ 2,\ \cdots,\ k$$

证明可以看数 $d=p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k}$ 确实为 a 与 b 的公因数，且易见一切 a 与 b 的公因数 d 必有 $p_1^{h_1}p_2^{h_2}\cdots p_k^{h_k}$的形式，其中$0\leqslant h_i\leqslant c_i(i=1,2,\cdots,k)$，故$d\leqslant d$。而得证$d=d^*(=(a,b))$。

这个结果很容易可以推广到a_1，a_2，…，a_s多个（$s\geqslant 2$）整数上去的。叙述与证法均可类似获得，此处从略。

任意给定两个自然数 a 与 b，怎样求出它的公因数 d 来呢？如果 a 是 b 的倍数，且$b>0$，则显然此时（a,b）$=b$。如果 a 不是 b 的倍数且$b>0$。则由带余除法，此时$r\neq 0$，有

$$a=qb+r,\ 0<r<b$$

那么很容易验有

$$(a,b)=(b,r)$$

实际上，可记$(a,b)=d^*$，$(b,r)=d'$ 记 $a=a^*d^*$，$b=b^*d^*$，以及$b=b'd'$，$r=r'd'$，那么有

$$d^*(a^*-qb^*)=r \Longrightarrow d^*|r$$

由$d^*|r$及$d^*|b$知$d^*|(b,r)$ 即 $d^*|d' \Longrightarrow d^* \leqslant d'$。另方面，也有

$$a=(qb'+r')d' \Longrightarrow d'|a$$

由$d'|a$,及$d'|b$知$d'(|a,b)$即 $d'|d^* \Longrightarrow d' \leqslant d^*$，从而$d'=d^*$。

因此，如果a，b 两整数，若 $a>b>0$，则求 a 与 b 两个数的最大公因数问题，经上述两点，总可转化为要么是b，要么是求 b 与 r 两数的最大公因数，也即只需对不超过 b 的两数求最大公因数即是，同样的思想方法，为求 b 与 r 两数的最大公因数，这就可转化为对不超过 r 的两数来求最大公因数即是，每转化一次，要么已经求到（整除），要么总至少原数减 1（带余除法，$0<r \leqslant b-1$），如此下去，有限步总可求得最大公因数的，所以这种用带余除法的辗转使用是求最大公因数的一个有效的方法。

例如$a=1859$，$b=1573$，我们可以把这种带余除法反复运用，有如下式子及结果：

1	1859	1573	5	(1859,1573)
	1573	1430		=(1573,286)
2	286	143		=(286,143)
	286			=143
	0			

现在我们把这种带余除法的辗转进行的过程书写如下。

已知 a 与 b 为整数，其中$b>0$. 在作如下带余除法过程中，若已整除了，则除法就此终止，若除不尽时，则继续进行，但有限步必然终止：

$$\begin{cases} a=bq_1+r_1, & 0<r_1<b, \\ b=r_1q_2+r_2, & 0<r_2<r_1, \\ r_1=r_2q_3+r_3, & 0<r_3<r_2, \\ \cdots\cdots\cdots\cdots & \\ r_{n-2}=r_{n-1}q_n+r_n, & 0<r_n<r_{n-1}, \\ r_{n-1}=r_nq_{n+1}\ (r_{n+1}=0) & \end{cases}$$

(4.7)

定理4.5 若a，b是任意两个整数($b>0$)，则 a 与 b 的最大公因数就是(4.7) 中最后一个不等于零的余数。

即

$$(a,b)=r_n \tag{4.8}$$

证明 由上面所述，有

$$\begin{aligned}(a,b) &= (b,r_1) = (r_1,r_2) = (r_2,\ r_3) = \cdots\\ &= (r_{n-3},\ r_{n-2}) = (r_{n-2},\ r_{n-1})\\ &= (r_{n-1},\ r_n) = r_n\end{aligned} \qquad \square$$

这个连续采用带余除法的式子(4.7)，一般称为辗转相除法。我们简称它为长除法。这种算法是我国古代数学家所创造的，中国古算学书中称为大衍求一术，外文书籍里，常把它叫做欧几里得（Euclid）除法。“求一术”在《九章算术》里以及“欧氏除法”在《几何原本》里出现，均在大约公元前二三百年之时，而《九章算术》与《几何原本》均是世界史上的两大传世杰作，它对数学的研究与发展在历史上曾起过巨大的促进作用。

既然（4.7）中出现的$r_n=(a,b)$，而根据定理4.1应当有$r_n=d_0$，即存在两整数x_0，y_0使得$r_n=ax_0+by_0$。实际上，长除法（4.7）本身就提供了求x_0，y_0的具体办法。

从（4.7）里的最末第二式，可以看到r_n为r_{n-1}与r_{n-2}的线性组合（$r_n=r_{n-2}-r_{n-1}q_n$），而r_{n-1}又为r_{n-2}与r_{n-3}的线性组合，故而r_n为r_{n-2}与r_{n-3}的线性组合；再……如此下去；r_n为r_2与r_1的线性组合，然而r为r_1与b的线性组合，最终便有r_n为a与b的线性组合。即存在x_0与y_0使$r_n=ax_0+by_0$。

为把寻找x_0与y_0的步骤写得更为具体规律些，我们对（4.7）有如下规律：

定理4.6 若a，b为两个正整数，则有

$$Q_k a - P_k b = (-1)^{k-1} r_k \quad (k=1, 2, \cdots, n) \tag{4.9}$$

其中

$$\begin{cases} P_0 = 1, \ P_1 = q_1, \ P_k = q_k P_{k-1} + P_{k-2} \\ Q_0 = 0, \ Q_1 = 1, Q_k = q_k Q_{k-1} + Q_{k-2} \end{cases} \tag{4.10}$$

证明 当$k=1$时，（4.9）显然成立。当$k=2$时，

$$r_2 = -[aq_2 - b(1+q_1q_2)]$$

但

$$1 + q_1q_2 = q_2P_1 + P_0,$$

$$q_2 = q_2 \cdot 1 + 0 = q_2Q_1 + Q_0$$

故

$$Q_2a - P_2b = (-1)^{2-1},$$

$$P_2 = q_2P_1 + P_0, \ Q_2 = q_2Q_1 + Q_0$$

假定（4.9）与（4.10）对于不超过$k(\geqslant 2)$的正整数都成立。今考察$k+1$时的情形，有

$$\begin{aligned}(-1)^k r_{k+1} &= (-1)^k (r_{k-1} - q_{k+1} r_k) \\ &= (Q_{k-1}a - P_{k-1}b) \\ &\quad + q_{k+1}(Q_k a - P_k b) \\ &= (q_{k+1}Q_k + Q_{k-1})a\end{aligned}$$

$$-(q_{k+1}P_k + P_{k-1})b$$

故而

$$Q_{k+1}a - P_{k+1}b = (-1)^k r_{k+1}$$

其中

$$P_{k+1} = q_{k+1}P_k + P_{k-1}$$

$$Q_{k+1} = q_{k+1}Q_k + Q_{k-1}$$

由归纳法，定理得证。 □

作为定理4.6的推论，我们有（4.8）中的r^n满足下列结论：

定理4.7 对于任意两个正整数 a，b 而言，存在整数x_0，y_0使得

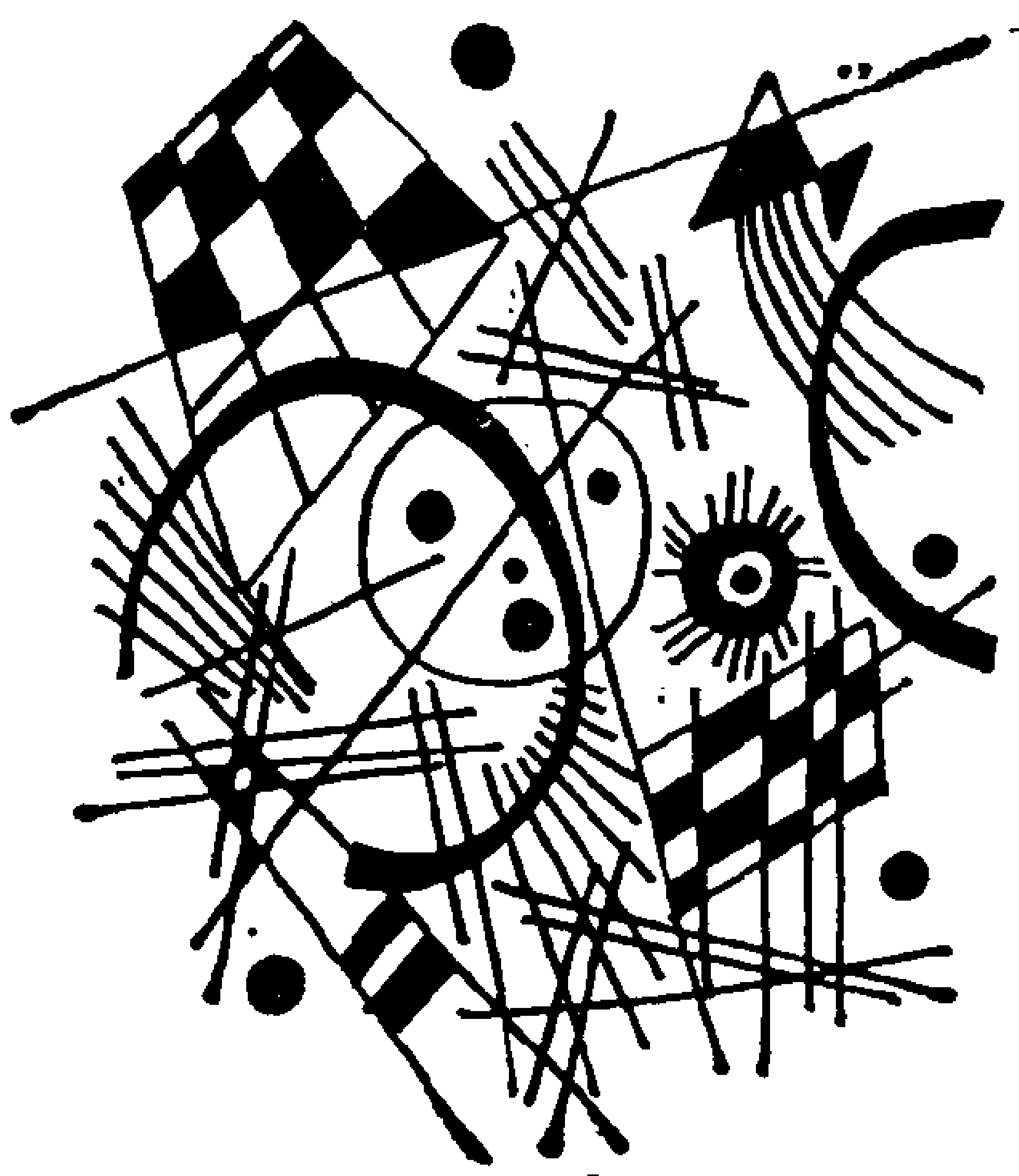
$$r_n = ax_0 + by_0$$

其中

$$x_0 = (-1)^{n-1}Q_n, \quad y_0 = (-1)^n P_n$$

而P_n与Q_n满足（4.10）的递推关系。

五 长除法与连分数



我们现在再回顾当初用阿基米德原理量(liáng)长度时，两个长度的比较过程，由人们的常识可知，例如当其中一个叫1尺时，另一个是它的多少倍便是多少尺。在这儿，数（shǔ）出的倍数是一个基本的数（shù）。但不一定总是那么正好量尽的，例如3尺与2尺长两杆子，并不正好量到头。我们说它是3尺为2尺的1.5倍，这里面就有个比例问题。譬如13:4是什么意思呢？我们可以理解成两个线段之比，一个是13寸（1尺3寸）另一个是4寸。所谓13:4是一个比值 $=3\frac{1}{4}$（或说3.25)，它表示：用4寸长的线段去量1尺3寸的线段，量3次有剩。将剩下的再反过来量4寸的（用短的量长的），量4次量完，说明剩下来的那个零头是四分之一，故说共

有$3\frac{1}{4}$倍，或说皆用1寸（公共单位）去量，一个13倍，一个4倍，其比为13:4。当然，一般地说，有公共单位的而长度之比必为有理数（所谓有理数r是指形如$\frac{n}{m}$的数，其中m，n为整数且$m \neq 0$），这是因为：如果两线段l_1与l_2有公共单位为e，皆能被长度e所量尽，它即有$l_1 = m_1 e$，$l_2 = m_2 e$，$(m_1 > 0, m_2 > 0)$那么$l_1 : l_2 = m_1 e : m_2 e = \frac{m_1}{m_2} = r$为一有理数。反之，假若$l_1$与$l_2$之比为一有理数的话，则必存在公共单位$e$，事实上，如果$l_1 : l_2 = r = \frac{n}{m}$，那么将$l_1$与$l_2$分别等分成$n$与$m$段，则必有$\frac{l_1}{n} = \frac{l_2}{m}$记此小线段为$e$，此即所求公共单位长。两个线段$a$与$b$，如果有一个公共单位线段$e$能同时量尽两者的话，称为是“有公度”的。因此我们说明了：凡两线段有公度的话，其长度比值必为有理数，且反之也对。

那么是不是任意两线段，总有公度呢？这在古希腊时代、纪元前4世纪半，以有个名叫德漠克利特(Democritus)的为代表的一些人，总认为是永远有公共单位的，也即任意两线段其长度之比认为是一有理数，这就是所谓数学中的“原

子"论派。但没有多久便发现这观点错了。这一点，在他同时代的一个叫欧朵克斯（Eudoxus）的创建了"比例论"，里面就曾有所指明。事实上，无公度的线段是存在的。

现在来看一个简单的例子：考虑一个大家颇为熟悉的平面几何图形——边长为 $OP_0=1$ 的正方形。研究其对角线OP的长度，由勾股定理，大家已知是 $OP=\sqrt{2}$（$OP^2=OP_0^2+P_0P^2=2$，见图5.1），记

$$\frac{OP}{OP_0}=x$$

这个比值 $x=\sqrt{2}$，但"$\sqrt{2}$"究竟是个什么数呢？OP与OP_0有公共单位长度吗？这个比值x（="$\sqrt{2}$"）真是有理数吗？下面我们还是用通过量（liáng）的办法看一看量出来的比数：

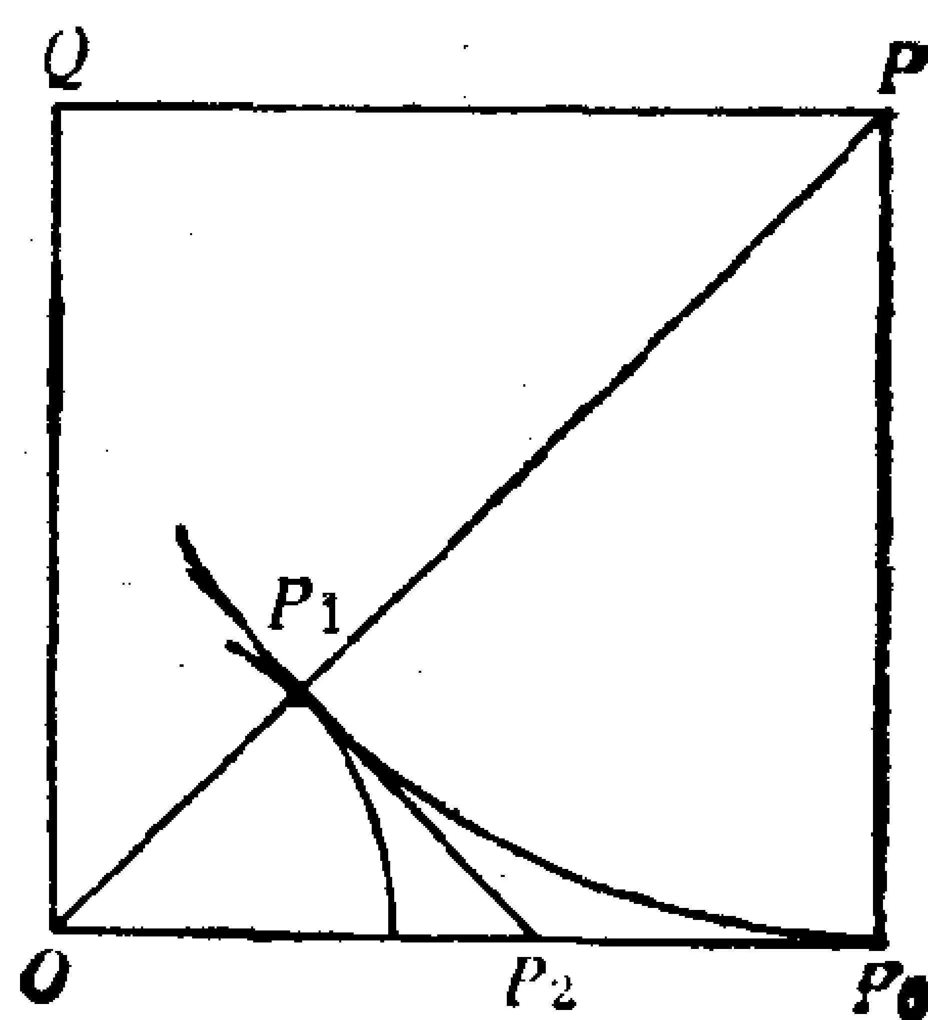


图 5.1

先用 $OP_0=P_0P$（见图5.1）来量OP得PP_1余OP_1，再用OP_1量OP_0，这时可过 P_1 作P_1P_2与OP相垂直交OP_0 于P_2，有（共交点的切线段）

$$OP_1=P_2P_1=P_2P_0$$

于是用OP_1 量OP^0 的问题，就化为了用OP_1 来量OP_2的问题．此时情况正如同一开始由OP_0 量OP时性质一样，即由直角边量对角线，可以进行同样手续反复量、余，并注意到x是正方形的对角线与直角边之比，有：

$$OP=1\cdot OP_0+OP_1$$

$$OP_0=1\cdot OP_1+OP_2$$

$$x=\frac{OP}{OP_0}=1+\frac{OP_1}{OP_0}=1+\cfrac{1}{\cfrac{OP_0}{OP_1}}$$

$$=1+\cfrac{1}{1+\cfrac{OP_2}{OP_1}}=1+\frac{1}{1+x}$$

这就是说，x是具有这样性质的的数（shù）：它加上 1 的倒数，再加 1 恰好就是它自已．我们若将这样的x反复运用、替代——或者说：反复地应用上法量来量去，一直量下去就可发现我们的记录本上出现了一系列如下形式的关系：

$$x=1+\frac{1}{1+x}$$

$$x=1+\cfrac{1}{1+\left(1+\cfrac{1}{1+x}\right)}=1+\cfrac{1}{2+\cfrac{1}{1+x}}$$

$$x=1+\cfrac{1}{2+\cfrac{1}{1+\left(1+\cfrac{1}{1+x}\right)}}$$

$$=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+x}}}$$

……………………………………………………

$$x=\cdots\cdots=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cdots\cdots}}}$$

对于上面右端那样的冗长公式，我 们 称 它 为一个“连分数”。如果我们在第 n 个加号处割断，且记

$$x_n=1+\cfrac{1}{2+\cfrac{1}{2+\ddots+\cfrac{1}{2+\text{[redacted]}}}}\quad (n-1)\text{个}$$

$$=1+\cfrac{1}{2+\cfrac{1}{2+\ddots+\cfrac{1}{2}}}\quad \left.\right\}(n-1)\text{个}$$

其中[redacted]表示割下去的部分，那么有

$$x_1=1$$

$$x_2=1+\frac{1}{2}=\frac{3}{2}=1.5$$

$$x_3=1+\cfrac{1}{2+\cfrac{1}{2}}=\frac{7}{5}=1.4$$

$$x_4=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}=\frac{17}{12}=1.417$$

$$x_5=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}}=\frac{41}{29}=1.414$$

……………………………………………

它与数值$\sqrt{2}$（=1.4142136……）越来越接近.

那么，数x(="$\sqrt{2}$")究竟是一个什么数呢？它并不是一个有理数！也就是说正方形的对角线长OP与一边长OP_0是不可公度的，它们之间是没

有公共单位长度的，其比值 x 是一个无理数。现在我们用反证法来证实这一点，即假设它们有公度——公共单位为 e，有

$$OP = pe, OP_0 = qe$$

此处 p 与 q 为正整数，则将引出矛盾。如下：

首先我们不妨假设 p 与 q 没有公因数，因为否则，若有公因数 d，而 $p = p'd$, $q'd$，其中 p' 与 q' 无公因数的话，此时可写

$$OP = p'de = p'e'(e' = de)$$

$$OP_0 = p'de = p'e'$$

此处已改选 $e' = me$ 为新公共单位了。所以，今不妨写

$$x = \frac{OP}{OP_0} = \frac{pe}{qe} = \frac{p}{q} \quad (p, q) = 1$$

其中 $(p,q) = 1$ 表示 p 与 q 是互素的（无任何大于或等于 2 的公因数）。再注意到：关系式

$$x = 1 + \frac{1}{1 + x}$$

中，当然 $x > 0$，它又可改写成 $x(1 + x) = (1 + x) + 1$，也即有 $x^2 = 2$，因而

$$2 = x^2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2$$

于是 p^2 是一偶数，这就推出 p 本身必为偶数（否

则奇数的平方仍是奇数），记$p=2p_1$，p_1为正整数，于是得$2q^2=(2p_1)^2=4p_1^2$，从而$q^2=2p_1^2$，这说明q^2也是一偶数，同理推出q本身也必为偶数，记$q=2q_1$，q_1为一正整数。可见p与q均有2为其公因数，这与$(p,q)=1$相抵触。 □

我们从量长度谈起，举了一个正方形一边长与其对角线长之间量来量去，量出了一串连分数$x_1,x_2,x_3,x_4,x_5,\cdots$的例子。而通常被称为"开方根2"（$\sqrt{2}$）的那个数

$$x=\lim_{n\to\infty}x_n=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ddots}}}$$

还不是一个有理数。那么，连分数与有理数之间是不是存在着一种互不相容的关系呢？

分数

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots+\cfrac{1}{a_n}}} \qquad (5.1)$$

叫有限连分数，其中$a_k(k=1,2,\cdots,n)$为正整数。

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots+\cfrac{1}{a_n+\ddots}}} \tag{5.2}$$

就是一个无限连分数。这里我们要求整数 $a_k>0(k=1,2,3,\cdots)$，如此（5.2)叫做简单连分数。

有限连分数（5.1）可缩写为 $[a_1,a_2,\cdots,a_n]$，无限连分数(5.2) 可写为 $[a_1,a_2,a_3,\cdots]$。

显然，（5.1）用逐步通分法可得上下均为整数（或用归纳法，作有限次归纳），就有

定理5.1 每一个有限连分数，必是一个正有理数。

有趣的是，反过来也对，有

定理5.2 每一个正有理数，必可表为一个有限连分数。

证明 设有理数为$\frac{a}{b}$，其中整数 $a>0$，$b>0$。为表连分数，用长除法：

a 除以 b，商为 q_1余r_2，即

$$a=q_1b+r_2$$

如果$r_2\neq 0$，即 $0<r_2<b$；再用 b 除以r_2有商q_2余r_3，如此下去：

$$b = q_2 r_2 + r_3 (0 < r_3 < r_2)$$

$$r_2 = q_3 r_3 + r_4 (0 < r_4 < r_3)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

经有限次手续，直到恰好除尽为止，例如到第n步时，有（$0 < r_n < r_{n-1}$）

$$r_{n-1} = q_n r_n (r_{n+1} = 0)$$

至此，顺便提一下，此时的r_n便是a与b的最大公因数(为何？请查式子由下往上推即可见得)。因此，回忆到本题要求，就有

$$\frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{\frac{b}{r_2}} = q_1 + \cfrac{1}{q_2 + \cfrac{r_3}{r_2}}$$

$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cfrac{r_2}{r_3}}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{r_4}{r_3}}}$$

$$= \underbrace{\cdots\cdots\cdots}_{\text{有限步}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}$$

即有$\frac{a}{b} = [q_1, q_2, \cdots, q_n]$这就证实了定理5.2的正确性。

例5.1 用长除法，可将$\frac{105}{38}$写成有限连分数，如下：

$$[q_1,q_2,q_3,q_4,q_5]=[2,1,3,4,2]$$

$$\frac{105}{38}=2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{2}}}}$$

	b	a	
(q_2) 1	38	105	2 (q_1)
(q_4) 4	29 / 9 (r_3)	76 / 29 (r_2)	3 (q_3)
	8 / 1 (r_5)	27 / 2 (r_4)	2 (q_5)
		2 / 0 (r_6)	$(n=5)$

由定理5.1与定理5.2，可见凡两个线段，如果有公度的话，其比值必为一个有限连分数，而且反之也对。换句话说：一个正有理数就是一个简单有限连分数。一般而言，任意一个有理数就是一个有限连分数。

定理5.3 每一个正无理数，一定可展开成

一个无限简单连分数。

证明 在几何上将一个正无理数 α 可看成为长度是 α 的线段，它与已知单位长（=1）的线段之间无公度（其比值为 α）。今仍用长除法互相量余，并引进记号 $[t]$ 与 $\{t\}$ 分别表示取实数 t 的整数部分与小数部分 $(0\leqslant\{t\}<1)$，有

$$\alpha=q_1\cdot 1+a_1,\ q_1=[\alpha],$$

$$a_1=\{\alpha\}\ (0<a_1<1)$$

$$1=q_2\cdot a_1+a_2,\ q_2=\left[\frac{1}{a_1}\right],\ a_2=\left\{\frac{1}{a_1}\right\}$$

$$(0<a_2<a_1)$$

$$a_1=q_3\cdot a_2+a_3,\ q_3\left[\frac{a_1}{a_2}\right],\ a_3=\left\{\frac{a_1}{a_2}\right\}$$

$$(0<a_3<a_2)$$

$$a_2=q_4\cdot a_3+a_4,\quad q_4=\left[\frac{a_2}{a_3}\right],\quad a_4=\left\{\frac{a_2}{a_3}\right\}$$

$$(0<a_4<a_3)$$

…………………………………………

这是一个连分数形式：

$$\alpha=\frac{\alpha}{1}=q_1+a_1=q_1+\frac{1}{\frac{1}{a_1}}=q_1+\frac{1}{q_2+\frac{a_2}{a_1}}$$

$$=q_1+\cfrac{1}{q_2+\cfrac{1}{\cfrac{\alpha_2}{\alpha_1}}}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{\alpha_3}{\alpha_2}}}$$

$$=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{\cfrac{\alpha_2}{\alpha_3}}}}$$

$$=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4+\cfrac{\alpha_4}{\alpha_3}}}}$$

$$=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4+\ddots+\blacksquare}}}$$

其中■表示尚未明确是有限步还是无限步的意思。但可指出，如此量算继续下去，是永远填不满空框的。因此否则将是有限连分数，那么α将是有理数了，这是不可能的。因此α的连分数展开式中。必为一个无限的连分数。 □

定理5.4 每一个无限简单连分数，必是一个正无理数。

证明 考虑无限连分数（5.2），记其部分

连分数（5.1），我们把形如（5.1）即$[a_1, a_2, \cdots, a_n]$的有限连分数称为形如(5.2)即$[a_1, a_2, a_3, \cdots]$的第n个渐近连分数。那么，容易看出有

$$[a_1]=\frac{a_1}{1}, [a_1, a_2]=\frac{a_1a_2+1}{a_2}$$

$$[a_1, a_2, a_3]=\frac{a_3(a_1a_2+1)+a_1}{a_3a_2+1}, \cdots$$

均是有限连分数，因而是有理数。一般记成

$$[a_1, a_2, \cdots, a_k]=\frac{p_k}{q_k}(k=1, 2, \cdots, n)$$

这里

$$\begin{cases}p_1=a_1\\q_1=1\end{cases}\quad\begin{cases}p_2=a_2a_1+1\\q_2=a_2\end{cases}$$

$$\begin{cases}p_3=a_3(a_1a_2+1)+a_1=a_3p_2+p_1\\q_3=a_2a_3+1=a_3q_2+q_1\end{cases}$$

…；记$p_0=1$，$q_0=0$，则当$k\geqslant 2$时

$$\begin{cases}p_k=a_kp_{k-1}+p_{k-2}\\q_k=a_kq_{k-1}+q_{k-2}\end{cases}$$

成立。证明可用归纳法，设当$k\leqslant s-1$时成立，则

$$\frac{p_s}{q_s}=[a_1, a_2, \cdots, a_{s-1}, a_s]$$

$$=\left[a_1,a_2,\cdots,\underbrace{a_{s-1}+\frac{1}{a_s}}\right]$$

$$=\frac{\left(a_{s-1}+\frac{1}{a_s}\right)p_{s-2}+p_{s-3}}{\left(a_{s-1}+\frac{1}{a_s}\right)q_{s-2}+q_{s-3}}$$

$$=\frac{a_s(a_{s-1}p_{s-2}+p_{s-3})+p_{s-2}}{a_s(a_{s-1}q_{s-2}+q_{s-3})+q_{s-2}}$$

$$=\frac{a_sp_{s-1}+p_{s-2}}{a_sq_{s-1}+q_{s-2}}$$

此即表明$k=s$时成立，再注意到$k=1,2$时显然成立，故得证。由此也容易指出，有（也可用归纳法证得）：

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^k \qquad (k\geqslant 2)$$

$$p_kq_{k-2}-p_{k-2}q_k=(-1)^{k-1}a_k \quad (k\geqslant 3)$$

记

$$\alpha_k=\frac{p_k}{q_k},\quad k-1,2,3,\cdots$$

则有（也可看到 p_k与q_k是互素的，$k=1,2,\cdots$）

i）$\alpha_1,\alpha_3,\alpha_5,\alpha_7,\cdots,\alpha_{2m-3},\alpha_{2m-1},\cdots$为一串递增数列。理由是

$$\alpha_{2m-1}-\alpha_{2m-3}=\frac{p_{2m-1}}{q_{2m-1}}-\frac{p_{2m-3}}{q_{2m-3}}$$

$$=\frac{(-1)^{2m-2}a_{2m-1}}{q_{2m-1}q_{2m-3}}>0$$

$$(m=2,3,\cdots)$$

ii）$\alpha_2,\alpha_4,\alpha_6,\alpha_8,\cdots,\alpha_{2m-2},\alpha_{2m}\cdots$为一串递减数列。理由是

$$\alpha_{2m}-\alpha_{2m-2}=\frac{p_{2m}}{q_{2m}}-\frac{p_{2(m-1)}}{q_{2(m-1)}}$$

$$=\frac{p_{2m}q_{2(m-1)}-p_{2(m-1)}q_{2m}}{q_{2m}q_{2(m-1)}}$$

$$=\frac{(-1)^{2m-1}a_{2m}}{q_{2m}q_{2(m-1)}}<0$$

$$(m=2,3,4,\cdots)$$

iii）$\alpha_{2m-1}<\alpha_{2m}$ $(m=1,2,3,\cdots)$，理由：

$$\alpha_{2m}-\alpha_{2m-1}=\frac{p_{2m}}{q_{2m}}-\frac{p_{2m-1}}{q_{2m-1}}$$

$$=\frac{p_{2m}q_{2m-1}-p_{2m-1}q_{2m}}{q_{2m}q_{2m-1}}$$

$$=\frac{(-1)^{2m}}{q_{2m}q_{2m-1}}>0$$

$$(m=1,2,3,\cdots)$$

这样一来，有理数列$\{\alpha_n\}$在数轴上的位置排列如图5.2所示。容易算出相邻两渐近分数之间的差数δ_{2m}为

$$\delta_{2m}=a_{2m}-a_{2m-1}=\frac{(-1)^{2m}}{q_{2m}q_{2m-1}}$$

$$=\frac{1}{q_{2m}q_{2m-1}}$$

$$\leqslant\frac{1}{(2m-1)(2m-2)}\leqslant\frac{1}{4(m-1)^2}$$

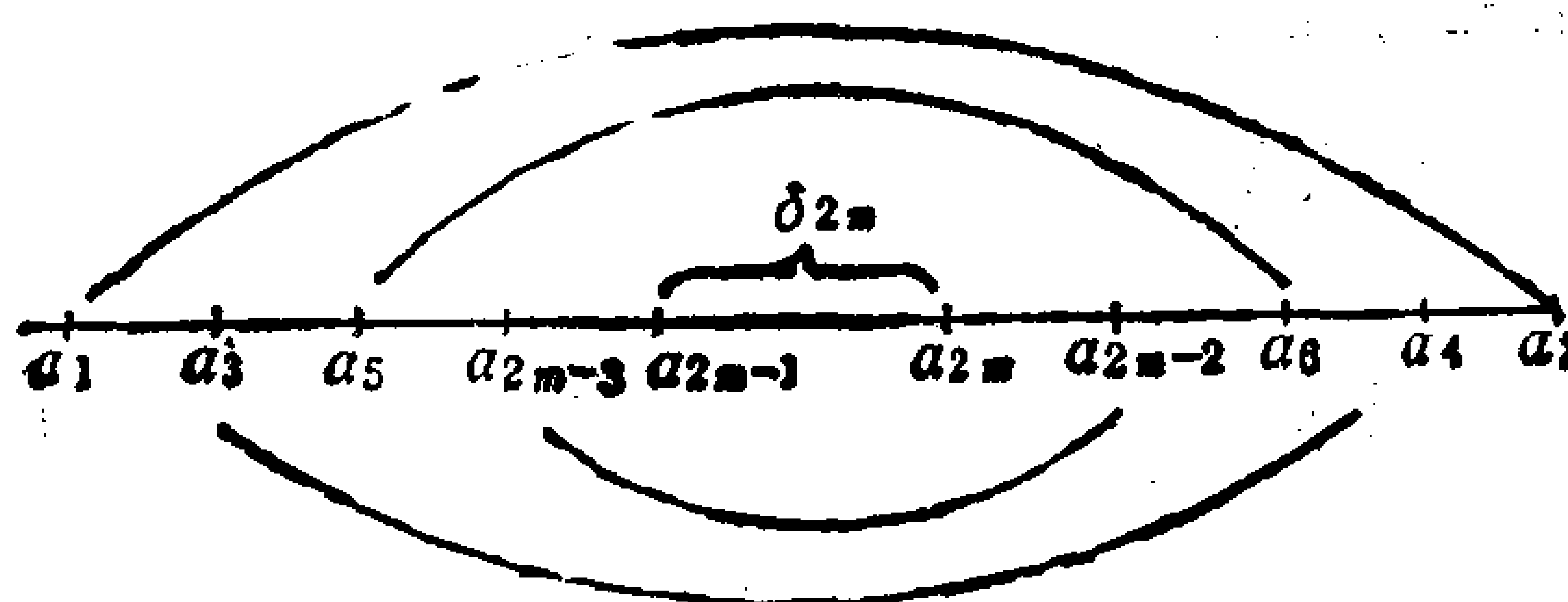


图 5.2

随着m的变大而迅速缩小（形成图 5.2 上所视区间成套，一个套住了一个的情形），其中我们已经用到了一个显然不等式（由于 $a_k\geqslant 1$）

$$q_k\geqslant q_{k-1}+1(k\geqslant 3)$$

由此得知：单数的 $\{a_{2m-1}\}$由左到右上升，双数的$\{a_{2m}\}$由右到左下降，两者间距δ_{2m}越来越小，当m很大时它很小 $\delta_{2m}\leqslant\frac{1}{4(m-1)^2}\to 0$（当$m\to\infty$）。因此单数与双数两个数列的极限相同，记其极限为$a$

$$a=\lim_{m\to\infty}a_{2m-1}=\lim_{m\to\infty}a_{2m}$$

因此

$$\alpha=\lim_{n\to\infty}\alpha_n=\lim_{n\to\infty}[a_1,a_2,\cdots,a_n]$$
$$=[a_1,a_2,\cdots]$$

这说明存在一个实数 α，它就是无限连分数 $[a_1,a_2,\cdots]$。这个数 α 当然是无理数，因为否则，它若是有理数则必为有限连分数了，矛盾.

例5.2 将 $\frac{1}{2}(\sqrt{5}+1)$ 展成连分数形式。

记 $\alpha=\frac{1}{2}(\sqrt{5}+1)$，因为 $[\alpha]=1$，故有

$$\alpha=1\{\alpha\}=1+\left\{\frac{1}{2}(\sqrt{5}+1)\right\}$$
$$=1+\frac{\sqrt{5}-1}{2}=1+\cfrac{1}{\cfrac{2}{(\sqrt{5}-1)}}$$
$$=1+\cfrac{1}{\frac{1}{2}(\sqrt{5}+1)}=1+\frac{1}{\alpha}$$

如此便有

$$\alpha=1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ddots}}}$$

这里还可以顺便指出一个有趣的结论：每一

个无限循环的连分数所表示的实数，一定是一个系数为整数的一元二次方程的根，而且反过来也对（详见：华罗庚《数论导引》第十章第六节的叙述）．

例5.3　$a=[1,2,1,2,1,2,1,\cdots]$

$$=1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\ddots}}}}$$

$$=1+\cfrac{1}{2+\cfrac{1}{a}}=1+\frac{a}{2a+1}$$

故而a满足一元二次方程 $2a^2=2a+1$，并注意$[a]=1$，从而$a>0$，解得$a=\frac{\sqrt{3}-1}{2}$。

从定理5.3与定理5.4知，任何一个正无理数就是一个简单（无限）连分数。一般地讲，任一无理数可看作就是一个无限连分数，当然，凡两个线段无公度的话，其充分且必要条件是它们的比值为一无理数——量、余所得的连分数必是一个无限连分数。

下面，我们来介绍一个很有用的“逼近定

理”：

从量长度的关系来看，凡两线段之间有公度还是无公度是有着本质的区别的，反映在两者间的比值上就是有理数与无理数的区别。但如果允许一定误差的话，两者之间是可以在某种意义下互相转化的，这就是所谓近似计算问题，这也是一个很实际有用的问题。因为随便一个实数α，在实际计算中不论是有理数还是无理数，总是用有理数来作（允许近似）计算的，而且习惯上常用有限位小数点的十进位计算法。我们主观上当然希望选用的有理数r来逼近实数α时，误差越小越好，如何选法呢？有趣的是，我们发现用连分数办法产生出来的有理数$\alpha_n=[a_1,a_2,\cdots,a_n]=\frac{p_n}{q_n}$是最好的近似分数，有所谓“最佳逼近定理”。确切地说，有

定理5.5 若α为任一实数，而$\frac{p_n}{q_n}$是α的连分数展开中第n个渐近分数，则在分母为$q\leqslant q_n$的一切有理数$\frac{p}{q}$中，$\frac{p_n}{q_n}$是α的最好的有理近似值。即：

$$\left|\alpha-\frac{p_n}{q_n}\right|\leqslant\left|\alpha-\frac{p}{q}\right|\quad（当q\leqslant q_n）$$

而且进一步地有

$$\left|\alpha-\frac{p_n}{q_n}\right| \leqslant \frac{1}{q_n q_{n+1}} \tag{5.3}$$

证明 只要检查一下我们对于定理5.4的证明过程，就会发现，对于不论什么正整数k，总有：实数α是夹在α_k与α_{k+1}这两者之间，也即有$|\alpha-\alpha_k| \leqslant \Delta_k$，其中

$$\Delta_k=|\alpha_{k+1}-\alpha_k|=\left|\frac{p_{k+1}}{q_{k+1}}-\frac{p_k}{q_k}\right|$$

$$=\frac{1}{q_k q_{k+1}}$$

只要令$k=n$就得(5.3)式。如今来考察当$q \leqslant q_n$时的任一有理数$\frac{p}{q}$，我们要证明：$\frac{p}{q}$这样的有理数点不落在由α_n与α_{n+1}所组成的一段之内部（见图5.3）。实际上，

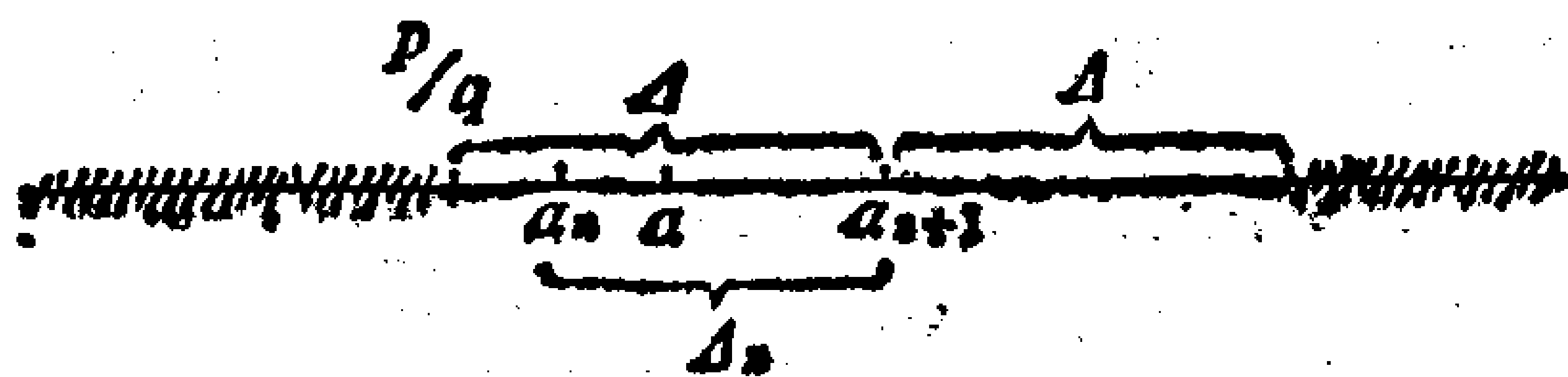


图 5.3

$$\Delta=\left|\frac{p}{q}-\frac{p_{n+1}}{q_{n+1}}\right|=\left|\frac{pq_{n+1}-p_{n+1}q}{qq_{n+1}}\right|$$

$$\geqslant \frac{1}{qq_{n+1}} \geqslant \frac{1}{q_n q_{n+1}} = \Delta_n$$

当然更有

$$\left|\frac{p}{q} - a\right| \geqslant | a_n - a |$$

这就证明了我们的最佳逼近定理是正确的。□

作为逼近定理的应用，我们举例如下：

例5.4 为什么四年一闰？每隔四年添一天，为什么第一百年又少闰一天？

这是因为：地球绕太阳一周需365天5小时48分46秒，也就是要

$$a^* = 365 + \frac{5}{24} + \frac{48}{24 \times 60} + \frac{46}{24 \times 60 \times 60}$$

$$= 365\frac{10463}{43200}$$

这么多天，如果每年按365天计算，久而久之，譬如43200年后，日子与实际就会相差10463天！这说明10463天应当在43200年中平均增配。但数字太大，计算不便，我们今用连分数来考察，有

$$a^* = [365,4,7,1,3,5,64]$$

$$= 365 + [0,4,7,1,3,5,64] = 365 + a$$

它的分数部分 a 的渐近分数是：

α_1	α_2	α_3	α_4	α_5	α_6
$\frac{1}{4}$	$\frac{7}{29}$	$\frac{8}{33}$	$\frac{31}{128}$	$\frac{163}{673}$	$\frac{10463}{43200}$

如今要说明几点：第一，如果我们采用 $365+\alpha_1$ 来代替 $365+\alpha$，此时 $\alpha_1=\frac{1}{4}$，那么显见每隔4年就应多出一天，这就是说四年一闰加一天，这是我们最初步的最佳渐近。第二，如果改用 $365+\alpha_2$ 来代替 $365+\alpha$ 就会更佳一些，此时 $\alpha_2=\frac{7}{29}$，那么每隔29年就应添7天，譬如说我们采用四年一闰，闰了七次之后休闰一年。当然，现在的历法并没有这样去算。第三，再看第三近似 $\alpha_3=\frac{8}{33}$，是说每33年中加8天，或即99年中加24天，这比原来前两者更精确。所以，如果四年一闰，那么正好100年加25天，然而不如99年加24天来得精确，故而在第一百年上少闰一天，以补 α_1，α_2 的误差出入，这样也比较方便实用。现在的历法就是第三近似，已相当精确了。当然，如果采用 α_4，α_5，最好是 α_6 就更佳，但由于数字过复杂不便实用，也就只用第三近似，并在后面加以

修正就是了，例如尚有四百年加一闰的说法等。

例5.5　圆周率π的连分数是

$$\pi = [3, 7, 15, 292, 1, 1, \cdots]$$

其渐近分数是

$$\frac{3}{1}, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102},$$

$$\frac{104308}{33215}, \cdots$$

因此我们看到在分母大小为10的左右那样分数里，挑一个有理数来近似于π的话，则$\frac{22}{7}$便是一切分母$\leqslant 7$中最好的一个分数。在古代，汉朝以来，曾一直粗用$\pi \approx \frac{3}{1}$，此乃第一近似，即古书所谓径一周三的说法，这当然是很不精确的。直到宋朝何承天（公元370—447年）提出用$\frac{22}{7}$来近似于π，这是连分数中第二近似值。后来，祖冲之（宋代，南北朝时代公元429—500年）提出用$\frac{355}{113}$来近似于π，这是π的连分数中，在分母为100上下时两个近似分数$\left(\frac{333}{106}与\frac{355}{113}\right)$中凡分母$\leqslant$113里最佳近似的一个（第4近似值）。祖冲之

还特地称何承天的$\frac{22}{7}$为疏率，而称他自己所发现的$\frac{355}{113}$为密率。若π用祖冲之的密率近似，则注意到渐近分数中$q_4=113$，$q_5=33102$等等，就有误差为

$$\left|\pi-\frac{355}{113}\right|\leqslant\frac{1}{q_4q_5}=\frac{1}{113\times33102}<\frac{1}{10^6}$$

故而$\frac{355}{113}$是π的精确到小数点六位的最佳有理近似值。事实上，祖冲之的$\pi\approx\frac{355}{113}=3.1415929$…，它与$\pi$的真值的前六位小数是符合的。可见祖冲之的成就是很突出的，他的密率$\frac{355}{113}$比后来西方人最早宣称用的$\frac{355}{113}$作为近似值的奥吐(Otto，1573年，德国人）要早一千多年！那么，当初祖冲之是不是已经应用了连分数基本理论呢？这个问题只有请数学史专家门去考证了！

六 素数的分布



既然早在二千多年前欧几里得就已经指出了全体素数在自然数中的个数是无穷多的。那么自然会问到：素数在自然数中的分布如何呢？例如是否每隔一定长度就会出现一个素数？那倒不见得。例如有如下定理：

定理6.1 任给自然数 $k>0$，总可找到正整数M，使得M，$M+1$，$M+2$，…，$M+k-1$ 连续k 个自然数均非素数。

证明 例如取$M=(k+1)!t+2$，当$t=1,2,3,\cdots$时，皆有M，$M+1$，$M+2$，…，$M+k-1$为复合数（因$M+l$中必有$l+2$因数，$1\leqslant l\leqslant k-1$）。 □

这个定理说明素数在自然数中"难得"出现的"稀"度状态。可是又有另一个情形：

定理6.2 假定 $n>2$，那么在 n 与$n!$之间一

定至少有一个素数。

证明 假定不超过n的全体素数为$p_1,p_2,\cdots,p_k$，又假定$Q=p_1p_2\cdots p_k-1$，由于$n>2$，所以$Q>4$，或者Q为素数，或者Q可以分解为若干素数的连乘积，故总存在素数$q\leqslant Q$（q为Q的素数因数），但q与$p_1,p_2,\cdots,p_k$显然均不相同，故$q>n$，另一方面$q\leqslant Q$，而$p_k\leqslant n$，故$p_{k-1}\leqslant n-1$，$\cdots$。因此

$$p_kp_{k-1}\cdots p_2p_1\leqslant n!$$

故而

$$q\leqslant Q\leqslant n!-1<n! \qquad \square$$

这个定理又表明素数在自然数中“必定”出现的“密”度状态。实际上，不仅对任何自然数$n\geqslant2$，在n与$n!$之间至少有出现一个素数，而且可以改进出现的间隔距离。例如有一个数学家叫贝特伦德(Bertrand)曾“猜想”在n与$2n$之间必有一个素数，这里$n\geqslant1$为任意实数。这件事被俄国数学家契贝晓夫（Чебышев）所证明。如下：

定理6.3（契贝晓夫——贝特伦德定理）对任一实数$x\geqslant1$，在x与$2x$之间必有一素数。

在证明这个契贝晓夫——贝特伦德定理之前，我们要先介绍两件事：第一，$n!$中含某素数

p 的方次数的计算问题。第二，关于 $(a+b)^n$ 的二项式展开中的系数性质的研究。

记号 $[y]$ 表示取不超过 y 的最大整数，而 $\{y\}$ 表示取 y 的零头部分（$\{y\}=y-[y]$）。例如：$[\pi]=3$，$[-\pi]=-4$，$\left[\frac{2}{3}\right]=0$，$\left[-\frac{3}{5}\right]=-1$，$\left\{-\frac{3}{5}\right\}=\frac{2}{5}$，$\{\pi\}=0.14159\cdots$，$\{\sqrt{2}\}=0.414\cdots$ 等等。这已在前面讲到长除法与连分数时曾经用到过。那么显然有：

Ⅰ. $y=[y]+\{y\}$,

Ⅱ. $[y]\leqslant y<[y]+1, y-1<[y]\leqslant y$,

$0\leqslant\{y\}<1$.

Ⅲ. $[n+y]=n+[y]$，若 n 为整数。

Ⅳ. $[x]+[y]\leqslant[x+y]$,

$\{x\}+\{y\}\geqslant\{x+y\}$.

Ⅴ. $[-y]=\begin{cases}-[y]-1, & \text{当 } y \text{ 不是整数时,}\\ -[y], & \text{当 } y \text{ 是整数时.}\end{cases}$

Ⅵ. 若 a,b 是两个整数，$b>0$，则

$$a=b\left[\frac{a}{b}\right]+b\left\{\frac{a}{b}\right\},\quad 0\leqslant b\left\{\frac{a}{b}\right\}\leqslant b-1$$

Ⅶ. 若 a,b 是任意两个正整数，则不大于 a 而为 b 的倍数的正整数的个数是 $\left[\frac{a}{b}\right]$.

以上这些性质是容易一一验证的，这里不再赘述。

我们将利用这一记号来论证$n!$中含指定素数p的最大方次数h为

$$h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right] \quad (6,1)$$

注意，若$p^t>n$，，则$\left[\frac{n}{p^t}\right]=0$，故上式只有有限项不为零，因而是有意义的写法。证明这个（6.1）式子是很容易的。因为可以设想把$2,\cdots,n$都分解成标准分解式，则由算术基本定理，h就是这$n-1$个分解式中p的指数之和。设其中p的指数是r的有n_r个$(1\leqslant r)$，则

$$\begin{aligned}h&=n_1+2n_2+3n_3+\cdots\\&=n_1+n_2+n_3+\cdots\\&\quad\ +n_2+n_3+\cdots\\&\qquad\quad\ n_3+\cdots\\&\qquad\qquad\ +\cdots\\&=N_1+N_2+N_3+\cdots\end{aligned}$$

其中

$$N_r=n_r+n_{r+1}+\cdots$$

恰好是$2,\cdots,n$这$n-1$个数中能被p^r除尽的个数，但由性质Ⅶ，$N_r=\left[\frac{n}{p^r}\right]$，故（6.1）成立，

因此，有写法

$$n! = \prod_{p\leq n} p^{\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$$

其中记号$\prod_{i=1}^{s} a_i = a_1a_2\cdots a_s$表乘积，而此处$\prod_{p\leq n}$表展布在不超过$n$的一切素数上的乘积式子。

如今再引进记号

$$C_n^k = \frac{n!}{(n-k)!k!}$$

实际上是从n个中取k个的组合个数，这个数中国数学史上称为贾宪数或叫杨辉数。它应当是整数。这是因为由性质Ⅳ用$n=(n-k)+k$，有

$$\left[\frac{n}{p^r}\right] \geqslant \left[\frac{n-k}{p^r}\right] + \left[\frac{k}{p^r}\right]$$

$$\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right] \geqslant \sum_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right] + \sum_{r=1}^{\infty}\left[\frac{k}{p^r}\right]$$

故

$$\prod_{p\leq a} p^{\sum_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right] + \sum_{r=1}^{\infty}\left[\frac{k}{p^r}\right]} \Bigg| \prod_{p\leq a} p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^r}\right]}$$

也即有$k!(n-k)!/n!$，整除性证得。

顺便说一下，$\frac{n!}{k!(n-k)!}=C_n^k$ 就是二项式 $(a+b)^n$ 展开的通项式的系数：

$$(a+b)^n=\sum_{k=0}^{n}C_n^k a^k b^{n-k}$$

这个系数很有规律，可排成三角形阵势：

						1						
					1		1					
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		5		10		10		5		1	
1		6		15		20		15		6		1

… … … … … … … …

中国数学史称杨辉三角形或说贾宪三角形。至迟在13世纪已被我国人民所发现。这要比欧洲最初发现这件事至少早 260 年左右，要比外国书上宣称的巴斯咯（Pascal）三角形（1654年）要早400 年以上。

例如尚有

$$C_n^k+C_n^{k+1}=C_{n+1}^k,\ (k=1,2,\cdots,n)$$

等性质，就不再一一多说了。

有了这些知识，我们现在可以来证明定理

6.3 这个契贝晓夫——贝特伦德定理了。准备分以下四步来阐明：

1）仍由二项式系数

$$C_{2n}^{n}=\binom{2n}{n}=\frac{(2n)!}{n!n!}$$

出发。但需要更精密的估计：当 $n\geqslant5$ 时，

$$\frac{1}{2n}2^{2n}<\binom{2n}{n}<\frac{1}{4}2^{2n} \qquad (\mathrm{i})$$

此式的左边的证明如下：

$$(2n)\binom{2n}{n}=\frac{2}{1}\cdot\frac{3}{1}\cdot\frac{4}{2}\cdot\frac{5}{2}\cdots\frac{2n-2}{n-1}$$

$$\frac{2n-1}{n-1}\,\frac{2n}{n}\,\frac{2n}{n}>2^{2n}$$

而右边则用归纳法。当 $n=5$时显然有

$$\binom{2n}{n}=252<256=\frac{1}{4}\cdot2^{10}$$

由于

$$\binom{2(n+1)}{n+1}=\frac{(2n)!(2n+1)(2n+2)}{(n!)^2(n+1)(n+1)}$$

$$<4\binom{2n}{n}$$

因此（i）成立。

2）命 $b\geqslant10$，以$\{\xi\}^*$表$\geqslant\xi$之最小之整

数，且命

$$a_1=\left\{\frac{b}{2}\right\}^*,\ a_2=\left\{\frac{b}{2^2}\right\}^*,\ \cdots,$$

$$a_k=\left\{\frac{b}{2^k}\right\}^*,\ \cdots$$

如此则

$$a_1\geqslant a_2\geqslant\cdots\geqslant a_k\geqslant\cdots$$

及

$$a_k<\frac{b}{2^k}+1=2\frac{b}{2^{k+1}}+1\leqslant 2a_{k+1}+1$$

由于两边都是整数，故得

$$a_k\leqslant 2a_{k+1} \tag{ii}$$

命m为最大之整数使得$a_m\geqslant 5$者。即$a_{m+1}<5$。又由(ii)式，$a_m<10$。因$2a_1\geqslant b$，故m个隔间

$$a_m<\eta\leqslant 2a_m,\ a_{m-1}<\eta\leqslant 2a_{m-1},$$

$$\cdots,\ a_1<\eta\leqslant 2a_1$$

整个地掩盖了隔间$10<\eta\leqslant b$。故有

$$\prod_{10<p\leqslant b}p\leqslant\prod_{a_1<p\leqslant 2a_1}p\prod_{a_2<p\leqslant 2a_2}p\cdots$$

$$\prod_{a_m<p\leqslant 2a_m}p$$

由于

$$\prod_{n<p\leqslant 2n}p<\binom{2n}{n}<2^{2(n-1)}$$

可知

$$\prod_{10<p<b} p \leqslant 2^{2(a_1-1+a_2-1+\cdots+a_m-1)}$$

$$<2^{2\left(\frac{b}{2}+\frac{b}{2^2}+\cdots+\frac{b}{2^m}\right)}<2^{2b} \qquad \text{(iii)}$$

3）以前已经证明：一素数 p 在$\binom{2n}{n}$中之幂数不大于 r，此 r 就是最大的整数使$p^r \leqslant 2n$者，由此可知素数 p 之大于$\sqrt{2n}$者其平方必不能整除$\binom{2n}{n}$.

尤可注意的是，当$n \geqslant 3$时适合于$\frac{2}{3}n<p \leqslant n$之素数 p 不能整除$\binom{2n}{n}$. 这是因为$3p>2n$，故在$(2n)!$的一切因数中仅有 p 及$2p$ 出现，而无其他之 p 的倍数。而$(n!)^2$中显然有因数 p^2。故如此之 p 不能数除$\binom{2n}{n}$. （这一点正是本证明中最主要之点）

总括以上所述，就得

$$\binom{2n}{n} \leqslant \prod_{p \leqslant \sqrt{2n}} p^r \prod_{\sqrt{2n}<p \leqslant \frac{2}{3}n} p \prod_{n<p \leqslant 2n} p$$

$$\leqslant \prod_{p \leqslant \sqrt{2n}} (2n) \prod_{\sqrt{2n}<p \leqslant n} p \prod_{n<p \leqslant 2n} p$$

由（i）及（iii）可知，当$n \geqslant 50$时（即$\sqrt{2n} \geqslant$

10时），

$$2^{2n}<(2n)^{\sqrt{2n}+1}\prod_{\sqrt{2n}<p<\frac{2}{3}n}p\prod_{n<p\leqslant 2n}p$$

$$<(2n)^{\sqrt{2n}+1}2^{\frac{4}{3}n}\prod_{n<p\leqslant 2n}p$$

若在n及$2n$间并无素数，则得

$$2^{2n}<(2n)^{\sqrt{2n}+1}2^{\frac{4}{3}n}$$

即

$$2^{\frac{2}{3}n}<(2n)^{\sqrt{2n}+1} \qquad \text{(iv)}$$

当n充分大时，此式显然不可能。今更具体地算出此式成立之确切范围。今用不等式$n\leqslant 2^{n-1}$（此式可用归纳法证之），

$$2n=(\sqrt[6]{2n})^6<([\sqrt[6]{2n}]+1)^6\leqslant 2^{6[\sqrt[6]{2n}]}$$
$$\leqslant 2^{6\sqrt[6]{2n}}$$

由（iv）可知（仍假定$n\geqslant 50$）

$$2^{2n}<(2n)^{3(1+\sqrt{2n})}<2^{\sqrt[6]{2n}(18+18\sqrt{2n})}$$

$$<2^{\sqrt[6]{2n}\times 20\sqrt{2n}}=2^{20(2n)^{\frac{2}{3}}}$$

即$(2n)^{\frac{1}{3}}<20$，$n<\frac{1}{2}\cdot 20^3=4000$，即(iv)式仅当$n<4000$时可能成立。故当$n\geqslant 4000$时必有一素数$p$适合于$n<p\leqslant 2n$。

4）当$n<4000$时可以具体验证如下：

2,3,5,7,13,23,43,83,163,317,

631,1259,2503,4001　　　　　　(Ⅴ)

乃一连串素数，后者小于前者之二倍，对任一n($1\leqslant n<4000$)可于（Ⅴ）中取得一最小素数p而大于n者。命p'为其前一项，则总有

$$p'\leqslant n<p\leqslant 2p'\leqslant 2n$$

故得定理6.3。

从定理6.1与6.3可以看出素数在自然数列中的分布是很不规则的，如果记$\pi(x)$为不超过x的素数个数，那么$\pi(x)$是x的怎样函数呢？有否很好的统计规律？或逻辑公式？关于这一点，是有一段很有趣的历史发展的。但要先介绍一下关于“对数”的这个概念。

大家知道若$a>0$，以及$x>0$，a^x就是一个指数形式。记

$$N=a^x$$

其中已知a，已知x，可求出N，此数称为：以a为底数，以x为指数的真数，若已知a，已知N反过来求x，这个x便称为：以a为底，以N为真数的对数，并重新记作

$$x=\log_a N$$

有一个数叫“e”是$\left(1+\frac{1}{n}\right)^n$等$n$很大很大

时，它的最终“极限”值，微积分中记为

$$e=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

其数值大约为$e\approx2.718\cdots$，这个数很重要，若以e为底取对数时往往这个“e”就不写了，例如

$$x=\log N$$

表以e为底的对数，称为自然对数若以10为底的对数，则称为常用对数，且记为

$$\lg N(=\log_{10}N)$$

有一个如下的不等式

$$\log\frac{n}{2}<\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}<\log n \quad (6.2)$$

是微积分中很基本简单的结果，这里就不打算详细地阐述了。如果记

$$H(n)=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$

那么由（6.2）即有

$$\log\frac{n}{2}<H(n)<\log n \qquad (6.2)'$$

它对所有$n>2$成立。

有了以上对于自然对数的认识，就可以稍稍介绍一下有关素数分布中，素数个数函数$\pi(x)$的一些历史进展了。

最早，大数学家高斯（Gauss）与勒让特（Legendre）曾用数值统计比较：

x	$\pi(x)$	$\frac{x}{\log x}$
1 000	168	145
10 000	1 229	1 086
50 000	5 133	4 621
100 000	9 592	8 686
500 000	41 538	38 103
1 000 000	78 498	72 382
2 000 000	148 933	137 848
5 000 000	348 513	324 149
10 000 000	664 579	620 417
20 000 000	1 270 607	1 189 676
90 000 000	5 216 954	4 913 897
100 000 000	5 761 455	5 428 613
1 000 000 000	50 847 478	48 254 630

发现了：$\pi(x)$与$\frac{x}{\log x}$之值当x很大时越来越接近，于是猜想：有没有当$x\to\infty$时，就有$\pi(x)$与$\frac{x}{\log x}$的比值就趋向于1：

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\log x}}=1 \tag{6.3}$$

在这方面首先获得重要结果的是契贝晓夫，他用初等方法证明了：

$$A\frac{x}{\log x}<\pi(x)<B\frac{x}{\log x} \tag{6.4}$$

对一切$x\geqslant 2$成立，其中A、B 为两常数，例如A取$\frac{1}{8}$，B取12等(实际还可更接近于1些)．关于这个不等式（6.4)，我们下面要给出一个简单的证明的，直到1896年，法国数学家哈德马(Hadamard)与普哇松(de la Vallee Poisson)才同时证明了这个高斯“猜想”（6.3)，史称素数定理，但他用到了很深的复变函数理论与方法，以后德国数学家魏纳（Wiener）给出了一个新的证明，避开了复变函数论，但方法中用到了高等数学分析，仍不初等，直到1949年，挪威数学家西尔贝格(Selberg)与匈牙利数学家艾多斯(Erdös)才分别同时给出了（6.3）以一个真正的初等证明。当然这个“初等”证明的内容也是相当繁长而且还是有一定的深难度的。顺便说一下，既然$\pi(x)$与$\frac{x}{\log x}$很接近，那么其误差项究竟有多大呢？这

方面有很多数学家作出了成绩，如苏联的丘达可夫（Чудаков），维诺格拉朵夫（И. М. Виноградов）以及英国数学家梯其玛西(Titchmarsh)等，我国数学家在研究有误差项的素数定理方面，对“三角和”这一方法作了很好的改进，有数学家华罗庚，闵嗣鹤，吴方，尹文霖（以及本书作者们）等诸位教授。当然该问题的研究，到现在还尚未彻底，具体的情况这里就不多谈了。

如今再顺便介绍一下契贝晓夫的这个不等式（6.4）的定理如下。

在证明此定理之前，需先确立如下二个引理：

引理1 当$k\geqslant 0$，

$$\pi(2^{k+1})\leqslant 2^k$$

证明 当$x>9$，有

$$\pi(x)\leqslant\frac{x}{2}$$

这是因为$\pi(x)$不会超过$\leqslant x$的奇数个数$\leqslant\frac{x}{2}$。另外，当$x\leqslant 9$时，显然由下列具体计算可得：

$$\pi(2)=1=2^0,\ \pi(4)=2=2^1,$$

$$\pi(8)=4=2^2$$

引理2 当$l>0$，

$$\frac{1}{2}l \leqslant H(2^l) \leqslant l$$

证明

$$H(2^l) = \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^{l-1}+1} + \cdots + \frac{1}{2^l}\right) \geqslant \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^l} + \cdots + \frac{1}{2^l}\right) = \frac{1}{2}l$$

$$H(2^l) = \left(\frac{1}{2} + \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) + \cdots + \frac{1}{2^l} \leqslant \left(\frac{1}{2} + \frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) + \cdots + \left(\frac{1}{2^{l-1}} + \cdots + \frac{1}{2^{l-1}}\right) + \frac{1}{2^l} \leqslant l$$

现在可以来证明这个定理（(6.4)式）了。为此，需先证

$$\prod_{n<p<2n} p \left| \binom{2n}{n} = \frac{(2n)!}{n!n!} \right| \prod_{\substack{p^r<2n \\ p^{r+1}>2n}} p^r \quad ①$$

因为：第一，在n与$2n$间的素数整除$(2n)!$，但不整除$n!$，故有上面的左式。第二，在$\binom{2n}{n}$中p的方次为

$$\sum_{m=1}^{r}\left(\left[\frac{2n}{p^m}\right]-2\left[\frac{n}{p^m}\right]\right)\leqslant r$$

因其中的每一项皆$\leqslant 1$。故得①式的右端。由①式可知

$$n^{\pi(2n)-\pi(n)}<\prod_{n<p\leqslant 2n} p\leqslant\binom{2n}{n}$$

$$\leqslant \prod_{p^r\leqslant 2n<p^{r+1}} p^r\leqslant(2n)^{\pi(2n)},n\geqslant 1 \quad ②$$

又因

$$\binom{2n}{n}=\frac{2n(n-1)\cdots(n+1)}{n(n-1)\cdots 1}$$

$$=2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{\nu}{n-\nu}\right)\cdots$$

$$\left(2+\frac{n-1}{1}\right)\geqslant 2^n$$

及

$$\binom{2n}{n}\leqslant(1+1)^{2n}=2^{2n}$$

故由②可知

$$n^{\pi(2n)-\pi(n)}<2^{2n},\quad 2^n\leqslant(2n)^{\pi(2n)},$$
$$n\geqslant 1 \qquad ③$$

命$n=2^k,k=0,1,2,\cdots$，可得

$$2^{k(\pi(2^{k+1})-\pi(2^k))}<2^{2^{k+1}},$$
$$2^{2^k}\leqslant 2^{(k+1)\pi(2^{k+1})},\quad k\geqslant 0$$

即得

$$k(\pi(2^{k+1})-\pi(2^k))<2^{k+1},$$
$$2^k\leqslant(k+1)\pi(2^{k+1}) \qquad ④$$

由引理1，

$$(k+1)\pi(2^{k+1})-k\pi(2^k)<2^{k+1}$$
$$+\pi(2^{k+1})\leqslant 3\cdot 2^k,\quad k\geqslant 0$$

令$k=0,1,\cdots,k$，而将所得之诸式相加，得

$$(k+1)\pi(2^{k+1})<3(2^0+2^1+\cdots+2^k)$$
$$<3\cdot 2^{k+1},\quad k\geqslant 0 \qquad ⑤$$

由④及⑤可知

$$\frac{1}{2}\frac{2^{k+1}}{k+1}\leqslant\pi(2^{k+1})<3\frac{2^{k+1}}{k+1},\quad k\geqslant 0 \qquad ⑥$$

命n为$\geqslant 2$的整数，取k使

$$2^{k+1}\leqslant n<2^{k+2},\quad k\geqslant 0$$

由引理2，得

$$\pi(n)\leqslant\pi(2^{k+2})<3\frac{2^{k+2}}{k+2}$$

$$\leqslant 6\frac{2^{k+1}}{H(2^{k+2})}\leqslant 6\frac{n}{H(n)} \qquad ⑦$$

及

$$\pi(n)\geqslant\pi(2^{k+1})\geqslant\frac{1}{2}\frac{2^{k+1}}{k+1}$$

$$=\frac{1}{8}\frac{2^{k+2}}{\frac{1}{2}(k+1)}\geqslant\frac{1}{8}\frac{2^{k+2}}{H(2^{k+1})}$$

$$\geqslant\frac{1}{8}\frac{n}{H(n)} \qquad ⑧$$

此对$n\geqslant 2$皆真。故有

$$\frac{1}{8}\leqslant\pi(n)\frac{H(n)}{n}<6 \qquad ⑨$$

再根据当$n\geqslant 2$时有（6.2）中关于$H(n)=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$的不等式：

$$\log\frac{n}{2}<\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}<\log n$$

以及当$n\geqslant 4$时有

$$\log\frac{n}{2}\geqslant\frac{1}{2}\log n$$

就可由⑨得：当$n\geqslant 2$时，有

$$\frac{1}{8} \leqslant \frac{\pi(n)}{\frac{n}{\log n}} \leqslant 12$$

在素数分布中，素数与自然数的关系，还能有更多的结论吗？全体素数，从2，3，5，7，11，…等开始，若顺次记为$p_1, p_2, p_3, \cdots$，请问第n个素数p_n是怎样的一个具体数字呢？也即有否公式$p_n = f(n)$来用n表示出素数p_n呢？目前为止并未找到。甚至能否有一个公式$g(n)$，当$n = 1, 2, \cdots$时，$g(n)$恒表素数（尽管它只是一部分素数），如今也没有办法。几百年前费马(Fermat)曾作公式

$$g(n) = 2^{2^n} + 1$$

他发现$g(0) = 3$，$g(1) = 5$，$g(2) = 17$，$g(3) = 257$，$g(4) = 65537$，皆为素数，从而猜想这是一个表示素数的公式了。但没多久，1732年数学家尤拉(Euler)正好举出

$$g(5) = 2^{2^5} + 1 = 641 \times 6700417$$

就并非素数。再退一步说，例如

$$g(n) = n^2 - n + 17$$

当$n = 0, 1, 2, \cdots, 16$时，全表示素数；

$$g(n) = n^2 - n + 41$$

当$n = 0, 1, 2, \cdots, 40$时，皆表示素数；而

$$g(n)=n^2-n+72491$$

当$n=0,1,2,\cdots$，11000时皆表示素数。虽然这些公式只是表示了有限个数，但就是连下面这样一个问题至今也尚未解决：任意给定一数N，可否求出一数p，当$n=0,1,2,\cdots$，N时，使得

$$g(n)=n^2-n+p$$

皆表示素数？甚至，在自然数中任取一正整数N，请问它是否为素数？怎样判别？到如今还没有一个有效的方法。例如在五十年代时，知道能写出来的最大素数为一个687位数$2^{2281}-1$，七十年代发现的更大素数是$2^{21701}-1$，尽管理论上已证明了素数个数是无穷的，但再大一些的具体素数就写不出来了。

又如前面已经说过贝特伦德曾“猜想”n与$2n$之间必至少有一个素数，这个猜想已被契贝晓夫所证明。但n^2与n^2+n之间是否必至少有一个素数呢？至今尚未解决。再如：

$3,5;5,7;11,13;17,19;29,31;\cdots;101,103;\cdots;10016957,10016959;\cdots;10^9+7,10^9+9;\cdots$

全是其差皆为2的素数对，称为孪生素数对。十万以内有1224对，百万以内有8164对孪生素数，五十年代时所知最大孪生素数对为

1000000009649,1000000009651

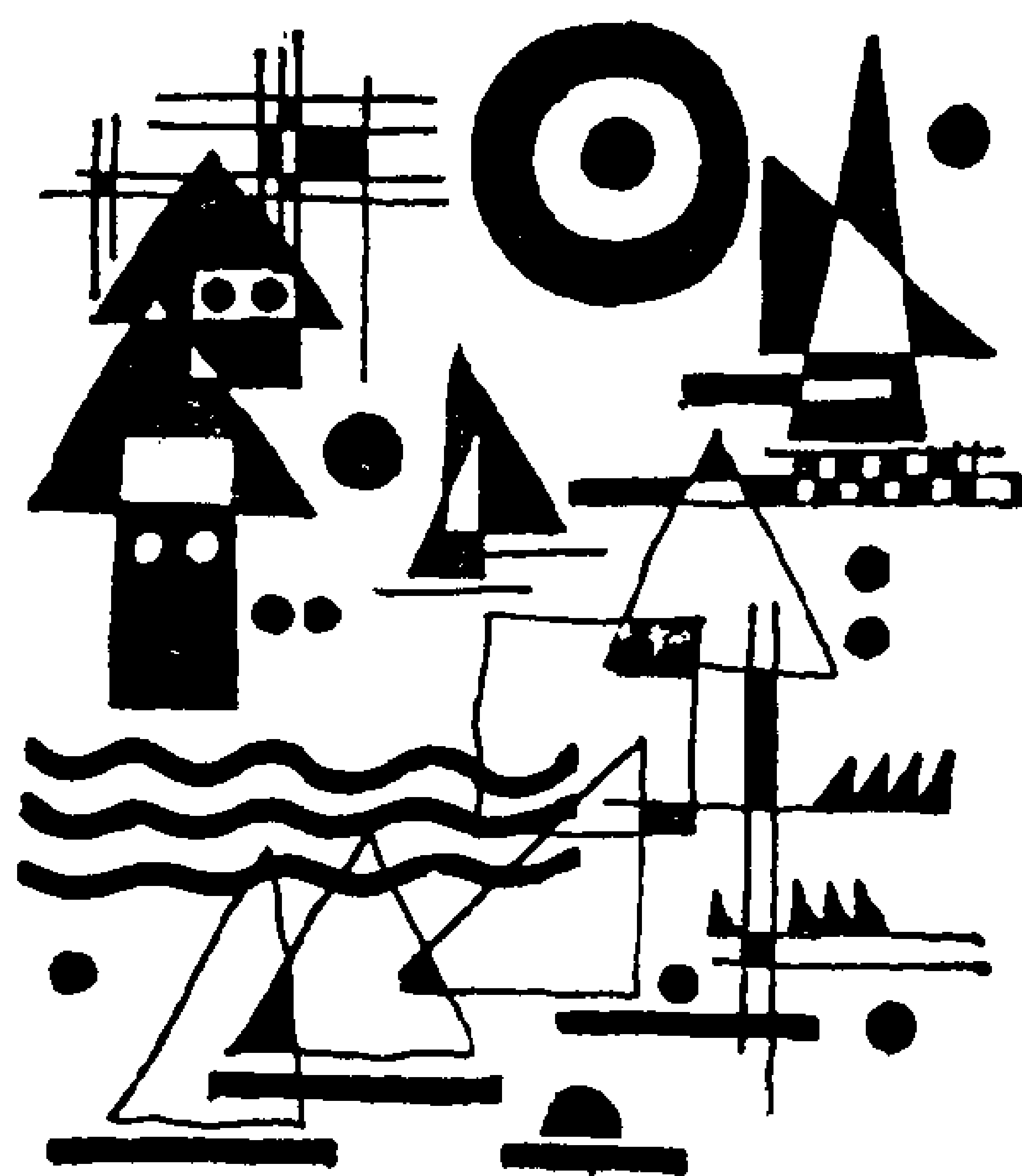
1976年威廉斯与察恩克(Willams and Zranke)发现了如今认识到的最大孪生素数对为

$$76\times 3^{169}-1,\ 76\times 3^{169}+1$$

但孪生素数的对数是否无穷多呢？也是一个至今仍未解决的世界难题。

所以说，在数论中，光围绕素数本身的了解上就产生了很多难题，可真谓群山起伏，有好多山头还需要我们去寻找道路。而哥德巴赫问题也是一个与素数密切相关的世界难题，它亦是数论中群山之一峰。攀登这个科学的山峰需要有不畏劳苦的精神。我国数学家王元、潘承洞以及本书作者之一（陈景润）等教授在已故导师华罗庚教授与闵嗣鹤教授等老一辈科学家的指导与支持关心下，在哥德巴赫问题研究中，曾攀登到了这座山峰接近最高处的境界，一些结果是走到了这个问题的世界最前列地步，但还是没有根本彻底解决哥德巴赫猜想是否真正成立的这一世界难题。

七 哥德巴赫的猜想



公元1742年6月7日德国人哥德巴赫(Goldbach)给当时住在俄国彼得堡的大数学家尤拉(或译为欧拉 Euler)写了一封信,问道：是否任何不比6小的偶数均可表示成两个奇数之和？同时也又问任何不比9小的奇数是否均可表成三个奇素数之和？我们把前者（偶数）称为问题（甲），后者（奇数）称为问题（乙）。同年6月30日尤拉复信写道:“任何大于6的偶数都是二个奇素数之和。虽然我还不能证明它，但我确信无疑地认为这是完全正确的定理”。也即下列问题是否正确应予论证：（甲）每一个偶数 $n\geqslant6$，均可找到两个奇素数p',p''，使得$n=p'+p''$;（乙）每一个奇数$n\geqslant9$，总可找到三个奇素数p_1,p_2,p_3，使$n=p_1+p_2+p_3$.这就是著名的哥德巴赫问题，或说是哥德巴赫猜想。

当然，如果（甲）成立的话，（乙）便随之成立，这是因为，任一奇数$N_{奇}=(N_{奇}-3)+3$，$N_{奇}\geqslant 9$，把其中$N_{奇}-3$这个偶数（>4），按（甲）（若成立的话），就有两个素数p_1，p_2，使得$(N_{奇}-3)=p_1+p_2$，而把3叫p_3（也是奇素数），便有了：

$$N_{奇}=p_1+p_2+p_3 \qquad (*)$$

这就指明了：若（甲）成立，则必有（乙）。但若（乙）成立，却反推不出（甲）来了。

整个19世纪结束时，哥德巴赫问题的研究没有任何进展。当然曾经有人作了些具体验证工作，例如$6=3+3$，$8=3+5$，$10=3+7$，$12=5+7$，$14=11+3$，$16=11+5$，$18=11+7$，…等等，现在已知直到33×10^6（三千三百万）以内的偶数都是对的，从而相应的奇数也有同样的结论。问题是较大的偶数怎么样？

本世纪初，数学家希尔伯特（Hilbert）在巴黎发表了著名23难题中，哥德巴赫问题曾被第8问题所涉及，1912年德国数学家朗道（Landau）在国际数学会报告中说，“即使要证明下面的较弱的命题：任何大于4的正整数，都能表成C个素数之和，这也是现代数学力所不能及的”。但是，本世纪数学迅速发展的事实，响亮地回答了

朗道的挑战，果然对问题（乙）与（甲）均取得了很大的成就。

人们遇到一些困难的理论问题时，总往往有两种方式去进行求解：一为直接地去求证本题的结论，即把诸如（*）这类式子理解为一个方程式，当p_1,p_2,p_3限制在素数范围内时，解答个数记为I（依赖于N），是否大于0呢？这方面就引出了对I进行估算的问题，最早对它进行研究的有英国数学家哈台与李德伍（Hardy and Litterword），成功地作出直接贡献的有苏联数学家维诺格拉朵夫和我国数学家华罗庚等人。另一方面的研究是将问题先削弱一些，然后逐步逼近而力争解决，这里头又分了两个途径：①弱型哥德巴赫问题：先将N写成一些素数的和：

$$N=p_1+p_2+\cdots+p_k \qquad (\text{I})$$

我们希望总有一种较好的分法，使得k越少越好，特别当N为偶数时，若能证明当$k=2$时有解（即有素数p_1，p_2使其和为给定的N），则原来的哥德巴赫问题（甲）就解决了。现在放宽来研究，当N给定之后，能作到怎样的k，使k个素数之和为N。这便是弱型哥德巴赫问题要研究的目标。②因数哥德巴赫问题：先将偶数N写成两个自然数之和：

$$N = n_1 + n_2 \qquad (\text{I})$$

而n_1与n_2里的素因数个数记为a_1与a_2，简记为（a_1，a_2）或写成“a_1+a_2”。这样的问题也可说是“殆素数问题”，即问：是否每一个充分大的偶数都可以表成两个殆素数之和？这里所谓“殆素数”就是指素因数的个数很少，例如不超过a个的那种整数也即希望有一种好的分法，使得（I）式中要求的a_1，a_2均不超过某指定数。注意，假若能证明对于每一个偶数N，总有$a_1=a_2=1$，也即有“1+1”结果的话，则哥德巴赫问题就成立了。

I、关于弱型哥德巴赫问题的研究

苏联数学家史尼尔里曼于1930年创造了“密率论”方法，结合1920年挪威人布尤创建的一种“筛法”，首先回答了朗道1912年在国际数学会上的著名挑战。他证明了下面一个重要的结果：每一个充分大的自然数都可以表为不超过k个素数之和，这里k是一个常数。这就开辟了弱型哥德巴赫问题研究的途径。后来有人明确估计出$k\leqslant 80$万，即在（I）中，当N充分大时，有k个素数使其和为N，而$k\leqslant 800000$，太大了！当然

是，最好：当N为偶数时，能证出$k\leqslant 2$，N为奇数时，能证出$k\leqslant 3$就根本解决了哥氏问题（甲）与（乙）。现在放宽研究k，希望k逐渐向2或3靠拢。这方面的研究成果，进展如下（表里的数字是k的上界）：其实最后一项结果，还可具体写为：偶数N时，$k\leqslant 18$，奇数N时，$k\leqslant 17$。

结　果	年　代	结　果　获　得　者
800000	1930	史尼尔里曼（苏联Шнирелбман）
2208	1935	罗曼诺夫（苏联Романов）
71	1936	海尔布朗（德国Heilbron） 朗道（德国Landau） 希尔克（德国Scherk）
67	1937	蕾西（意大利Ricci）
20	1950	夏彼罗（美国Shapiro） 瓦尔加（美国Warga）
18	1956	尹文霖（中国）
6	1976	旺格汉（R.C.Vaughan）

现在来谈谈史尼尔里曼的“密率”是怎么回事。由某些整数所组成的集合记为A，其中在$\leqslant n$内出现的全体元素记为$A(n)$，如果存在正数$\alpha_1>0$，使得对一切n均有$A(n)\geqslant\alpha_1 n$的话，亦即有

$$\frac{A(n)}{n}\geqslant\alpha_1$$

此时说A的密度为α_1，显然$\alpha_1\leqslant1$，如果能找到一个最大的$\alpha>0$使得

$$\frac{A(n)}{n}\geqslant\alpha$$

对一切自然数n成立的话，则称这个正数α为A的密率。

若记集合$A=\{a_1,a_2,\cdots\}$，如果：$a_1>1$，则显然A的密率为0；当$a_n=1+r(n-1)$，$(r>0)$，即首项为1，公差为r的等差序列时，则A的密率为$\frac{1}{r}$；但每一个等比序列所成集合的密率是0；由素数定理或契贝晓夫定理知全体素数集合P的密率为0；只有当A为全体自然数时其密率为1，而且反过来也对：当A的密率为1时，A就是全体自然数的集合。

史尼尔里曼首先给出了下列定理：

定理7.1 设A, B是两个集合，A, B的密率分别为α，β，记$C=A+B$表示C的元素由A内元素与B内元素的和组成*，而C的密率为γ，则有

$$\gamma \geqslant \alpha+\beta-\alpha\beta$$

证明 为方便起见，我们把集合A的密率α记为$\alpha=d(A)$。其余记号类似．用集合记号法，有$C=A+B$，而

$$A(n)=\sum_{\substack{1\leqslant a\leqslant n\\ a\in A}}1,\quad B(n)=\sum_{\substack{1\leqslant b\leqslant n\\ b\in B}}1,$$

$$C(n)=\sum_{\substack{1\leqslant c\leqslant n\\ c\in C}}1,$$

$$d(A)=\alpha,\quad d(B)=\beta,\quad d(C)=\gamma$$

那么，在自然数的一段$(1,n)$中含有A内的$A(n)$个整数．设用a_k及a_{k+1}表其中依次相邻的两个数，则在这两数之间有$a_{k+1}-a_k-1=l$个数不属于A，它们是

$$a_k+1, a_k+2, \cdots, a_k+l=a_{k+1}-1$$

以上各数中间凡可以写成$a_k+b(b\in B)$这种形式的数都属于C的，它们的个数等于B在$(1,l)$一段中所包含整数的个数，这当然是$B(l)$。

---

* 可用记号：$C=\{a_i+b_j|a_i\in A,\ b_j\in B\}$。

因此，在A的每相邻两数之间，如果所包含的一段自然数的长度（即个数）是l，就至少有$B(l)$个数属于C。因此在自然数的一段（1，n）中，C所包含整数的个数$C(n)$至少是

$$A(n)+\Sigma B(l)$$

上式中Σ的各项通过$(1,n)$中不含A内整数的一段一段的自然数。但根据密率的定义，有$B(l)\geqslant \beta l$，故

$$C(n)\geqslant A(n)+\beta\Sigma l$$
$$=A(n)+\beta\{n-A(n)\}$$

上面最后一个等式的成立是由于Σl等于$(1,n)$中不落在A内的整数的个数，当然它等于$n-A(n)$。又由$A(n)\geqslant \alpha n$，故

$$C(n)\geqslant A(n)(1-\beta)+\beta n\geqslant \alpha n\cdot(1-\beta)+\beta n$$

由此立刻得到

$$\frac{C(n)}{n}\geqslant \alpha+\beta-\alpha\beta$$

上式对所有整数n都成立，故

$$\gamma=d(C)\geqslant \alpha+\beta-\alpha\beta \qquad (7.1)$$

由这个不等式（7.1），还可以引出一个重要的结果：

定理7.2 若$C=A+B$，而$d(A)+d(B)\geqslant 1$，

则必有 $d(C)=1$，（也即此时C必为全体自然数集合）。

证明 我们首先指出，如果

$$A(n)+B(n)>n-1$$

则有$n\in A+B$，事实上，若n在A或B中，则定理已成立。今设n既不在A又不在B中，于是

$$A(n)=A(n-1),\quad B(n)=B(n-1)$$

而有

$$A(n-1)+B(n-1)>n-1$$

设在$(1,n-1)$一段内，A与B所包含的数分别为

$$a_1,a_2,\cdots,a_r$$

$$b_1,b_2,\cdots,b_s$$

则 $r=A(n-1)$，$s=B(n-1)$，而

$$a_1,a_2,\cdots,a_r$$

$$n-b_1,n-b_2,\cdots,n-b_s$$

都在$(1,n-1)$一段中，它们的总个数是 $r+s=A(n-1)+B(n-1)>n-1$ 所以其中至少有两个相等，使得

$$a_i=n-b_k$$

则$n=a_i+b_k$故n在$A+B$中。

注意

$$\frac{A(n)}{n}\geqslant d(A),\quad \frac{B(n)}{n}\geqslant d(B)$$

若$d(A)+d(B)\geqslant 1$，则有

$$A(n)+B(n)\geqslant n>n-1$$

此时$n\in C$，这对一切n成立。故C为自然数集合，定理7.2成立。

史尼尔里曼这个密率不等式定理

$$d(A+B)\geqslant d(A)+d(B)-d(A)\cdot d(B) \tag{7.1'}$$

为弱型哥德巴赫问题的进展奠定了基础。后来人们总想改进这个不等式（7.1)′。故在$d(A)+d(B)\leqslant 1$假设之下，有所谓朗道——史尼尔里曼的“假说”：

$$d(A+B)\geqslant d(A)+d(B) \tag{7.2}$$

推广一下，在$\sum_{i=1}^{k} d(A_i)\leqslant 1$条件下，有没有

$$d\left(\sum_{i=1}^{k} A_i\right)\geqslant \sum_{i=1}^{k} d(A_i) \tag{7.3}$$

成立？

当然，由（7.2）到（7.3）是很容易的。

这个假说最初是通过具体的例子，在1931年由史尼尔里曼和朗道推想出来的，看起来这个假说很简单其实很难证明。苏联数学家辛钦在$d(A_1)=\cdots=d(A_k)$的条件下，首先证得了这个假说成立。接着有不少的数学家企图证实这

个"假说"，但都只得到部分的结果。直到1942年，英国一位年轻的工程师名叫芒(Mann)的，在一次听报告时知道了这个问题，他回去后最终把这个不等式(7.2)证出来了，史称芒定理。1943年美国数学家阿丁（Artin）与德国数学家希尔克（Seherk）给出了比较简单的证明，1954年又由希尔克与刻姆剖曼（Kemperman）又给出了一个更新更简单的证明，并有所推广，成为后来数论教科书上的标准叙述。

对于弱型哥德巴赫猜想来说，由定理7.1与定理7.2就已足够。

事实上，如果一个集合A其密率为正密率$a>0$，则记

$$A_k=\underbrace{A+A+\cdots+A}_{k}\ (\text{共}k\text{项堆垒集合})$$

则可得

$$d(A_k)\geqslant 1-(1-a)^k$$

显然只要取k足够大时，就有$d(A_k)>\frac{1}{2}$，那么集合$C=A_k+A_k$就有

$$C(n)=A_k(n)+A_k(n)>\frac{1}{2}n+\frac{1}{2}n$$

$$=n>n-1$$

故$n\in C$，它对一切自然数n成立，故此时C就是全体自然数集合。

可惜的是全体素数集合P的密率恰巧为0，而并非正密率。但用布朗（Brun）筛法，可以获得集合$P+P$是正密率，从而若干个（例如s个）$P+P$就是全体自然数集合了。于是每一个自然数就可以写成$2s$个素数的和，这样弱型哥德巴赫问题的史尼尔里曼定理就成立了。当然，用筛法来证明$P+P$集合具有正密率时，可用1919年布朗筛法，也可用之后更好的1949年的西尔贝格（Selberg）筛法来推演的。无论那种筛法来证明$P+P$具有正密率这一结论时，均较复杂。这里就不再一一细叙了。

顺此，我们还要说明一下用筛法与单用密率方法在弱型哥德巴赫问题中的作用不同。例如用筛法与密率论相结合的方法可以证明充分大偶数能表素数和的定理。这“充分大”到底多大？往往是无法算出来的。如尹文霖证明每个充分大偶数可表至多18个素数的和，旺格汉进一步证明每个充分大偶数可表至多6个素数的和，均是对“充分大”的偶数而言的。单用密率的方法其优越之处是在于可以证明对所有正整数表素数和的定理。例如，1977年旺格汉证明了所有正整数均

可表为至多26个素数的和。1983年，我国张明尧博士改进为：所有正整数均可表为至多24个素数的和。

关于弱型哥德巴赫问题从史尼尔里曼到尹文霖以至旺格汉，以及再由旺格汉到张明尧的进展思路依据就介绍到这儿。但这里我们还特别应当提到下列一段重要的科学史实：曾在1922年，英国剑桥大学教授哈台与素德伍首创了“圆法”，也就是前面说到的，他们最早对哥德巴赫问题的解数 I 作了巧妙的估算。但后来联系哥氏问题求解时，却利用了一个“黎曼猜想”，在承认黎曼猜想成立的前提下，他证明了奇数哥德巴赫猜想（乙）成立。但是这个黎曼的假想，也是至今未曾解决的世界难题！所以这两位教授的工作有战斗之功劳，无胜利之成果。

1937年，古彼德堡即现在的列宁格勒城的一位数学家维诺格拉朵夫不用任何假设，创造了“三角和方法”的数学工具，在世界上第一个证明了大奇数哥德巴赫猜想正式成立，从而称为哥德巴赫——维诺格拉朵夫定理，或简称维氏定理：当$N_{奇}$充分大时，（乙）成立（例如1946年有人具体指出了：譬如当$N \geqslant e^{e^{16.038}}$—大约为 10的50万次方时，便有素数$p_1, p_2, p_3$使(*)成立)。

因此，在(Ⅰ)中，1937年已被维氏证明了：不论奇偶的大整数N，均有$k\leqslant 4$，或确切地说：当N为大奇数时，有$k\leqslant 3$；当N为大偶数时，有$k\leqslant 4$。这已经远比1950，1956诸年代的$k\leqslant 20$以及$k\leqslant 18$等结果来得优越得多了。那么，为什么还将落后于维氏1937年的结果加以重视赞扬呢？原因是：维氏用到了诸如复变函数换路积分等精深的复分析方法，但鉴于当初原问题是否能在实分析的限制中用“初等方法”予以求解呢？这在方法上也颇有特色的，此处表格中的结果全是在初等方法中获得的，因而也引人注目。

这里还应介绍一下，1959年潘承洞还将p_1，p_2，p_3限止在$\frac{N}{3}$附近时，作出了一个很好的估计。1977年潘承洞的弟弟我国数学家潘承彪曾对于原来维氏定理的维氏繁难的证明，给出了一个十分简化的很好证明。

特别应当提出的是：1938年华罗庚教授证明了几乎所有偶数都能表成两奇素数的和，也即哥德巴赫猜想几乎对所有偶数成立。这就为今天尚在研究的“例外值”课题，开辟了新的道路。早在1941年，华罗庚教授对维氏“三角和方法”作了非常深刻的研究与改进，并对维氏定理作了重

要推广，华罗庚教授证明了：每一个充分大的奇数N，皆可表为三个奇素数的k次方之和：

$$N=p_1^k+p_2^k+p_3^k \qquad (*)'$$

其中k为任意给定的正整数。特别，当$k=1$时，即维氏定理。

Ⅱ. 关于因数哥德巴赫问题的研究

尽管在哥德巴赫问题上已有弱性问题的一系列成果，以及尤其是维氏定理与华氏推广等优秀工作，但面临偶数的哥氏原猜想问题，并没有给予直接的根本的解决。

大奇数哥氏问题（乙）已为维氏所解决，大偶数哥氏问题（甲）怎么办？针对这一问题，在因数哥德巴赫问题的研究方面，逐步进展，有了一系列的成果。挪威数学家布尤在1920年创造一种“筛法”，首先证明了下面一个结果：每一个充分大的偶数都可以表示为两个各不超过9个素数相乘积的和，也即在（Ⅱ）中，当N为大偶数时，

$$N=p'_1\cdots p'_{a_1}+p_1''\cdots p_{a_2}''$$

其中p'，p''均表素数，而素因数个数$a_1\leqslant9$，$a_2\leqslant9$，即（9,9），或说证得了“9+9”。这在殆素数

问题研究上首开记录。之后便有接二连三的改进工作，特别是我国一些数学家在他们年轻的时候，成功地提出了利用“筛法”及“三角和方法”相结合的新解析数论方法，在五十年代到六十年代期间，作出了一系列重要的改进，取得了许多优秀的成果，在这基础上，本书作者之一（陈景润）曾于六十年代后期到七十年代初获得了“1+2”的重大结论，取得了世界领先的成果。关于这方面的研究进展情况如下表所示：

结　果	年代	结果获得者
(9,9)	1920	布龙（挪威Brun）
(7,7)	1924	雷特马赫（德国Rademacher）
(6,6)	1932	埃司特曼（英国Estermann）
(5,7),(4,9),(3,15),(2,366)	1937	蕾西（意大利Ricci）
(5,5)	1938	布赫夕太勃（苏联Бухштаб）
(4,4)	1940	布赫夕太勃（苏联Бухштаб）
(1,c),c常数	1948	瑞尼（匈牙利Renyi）
(3,4)	1956	王元（中国）
(3,3),(2,3)	1957	王元（中国）

续表

结　果	年代	结 果 获 得 者
(1,5)	1961 1962	巴尔班（苏联Барбан） 潘承洞（中国）
(1,4)	1962 1963	王元（中国） 潘承洞（中国） 巴尔班（苏联Барбан）
(1,3)	1965	布赫夕太勃（苏联Бухштаб） （小）维诺格拉朵夫 （苏联А.И.Винорабов） 波皮里（德国Bombiri）
(1,2)	1973	陈景润（中国）

这里应当说明的是巴尔班（1,4）结果，以及其1961年（1,5）的工作中，证明都有错误，经潘承洞教授在1964年指出后，到1970年他才给予改正。

这儿还要谈谈1948年匈牙利数学家瑞尼的“1+c”（c常数，很大）工作，这是很有意思的记录。因为这里开始了可以控制住一个为素数，而只要努力降低另一个的素因数个数就行了。这方面的研究，首先是王元于1957年在黎曼假设下证得了“1+5”成立。毋需任何假设的成果应当归

功于1962年潘承洞的“1+5”结果，这个结果第一次定量地而且是低记录地引向了接近“1+1”的境界。实际上，由1962年的“1+5”之后，1963，1965相继出现了“1+4”以及“1+3”的重要成就。以致于在1966到1973年内又出现了我们的最新成果“1+2”结论。顺便说一下，所谓结果是1966年到1973年完成，是指本书作者之一（陈景润）实际上已在1966年作出了这一结论，也曾用某些方式写过简报，但详尽而正式地写成论文发表（于《中国科学》杂志）乃是1973年，因此一般都说是在1973年获得的。在我们的文章发表后的短短几年中，世界上就出现了很多种简化的证明，其中有四、五个简化证明是较好的，其中最好的简单而本质的证明就是由我国数学家王元、丁夏畦与潘承洞三教授合作的论文中所给出。我们的结果“1+2”一发表，就曾引起了世界数学家的重视与兴趣，英国数学家哈伯斯坦姆和德国数学家黎希特合著的一本书叫《筛法》的数论专著，原有十章，付印后见到了我们的“1+2”结果，特为之增添写上了第十一章，章目为“陈氏定理”。所谓“陈氏定理”的“1+2”结果，通俗地讲，是指：对于任给一个大偶数N，那么总可以找到奇素数p'，p''或p_1，p_2，p_3，使得

下列两式至少有一个成立：

$$N = p' + p'' \qquad (\alpha)$$

$$N = p_1 + p_2 p_3 \qquad (\beta)$$

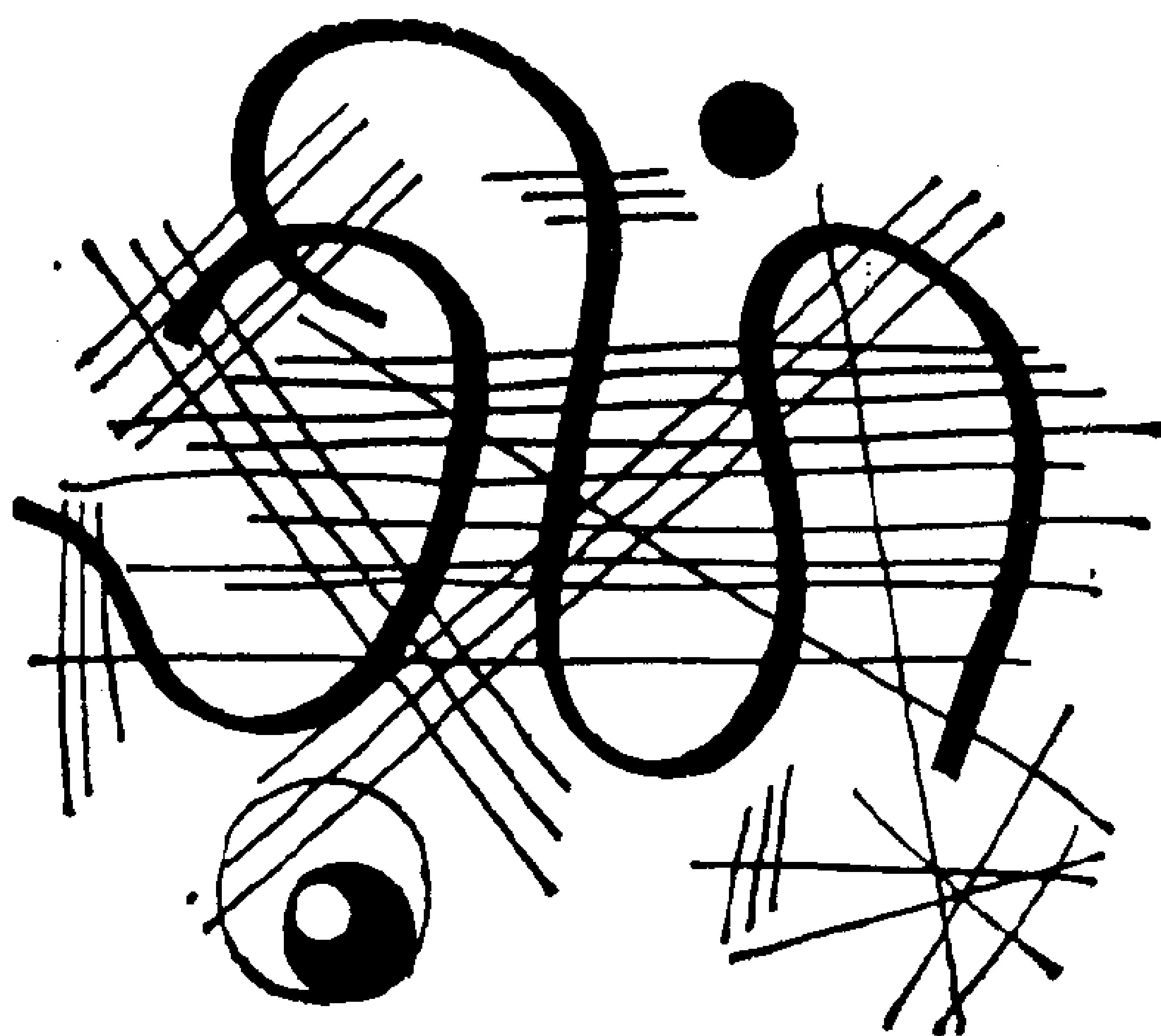
当然并不排除(α)、(β)同时成立的情形，例如在"小"偶数时，若$N = 62$，则可以有

$$62 = 43 + 19, \text{以及} \quad 62 = 7 + 5 \times 11$$

总的来说，哥德巴赫问题是我们科学群山之一峰，在数论中，或扩大一些说，在数学中群山耸立，不少科学的保垒确实需待我们去攻克，特别是期待着我们的青年数学工作者能够接过老一辈科学家的班而奋勇前进！上述进展表格中所列举的这一系列突出的成就，一方面固然是作者们不倦努力的结晶，另方面也更应该看到，这二、三十年来，以华罗庚教授为首的中国数论学派的发展壮大过程，许多青年数学家曾在老一辈科学家的辛勤培育下，共同努力，形成了一个数论研究的集体，这为奠定我们获得的"1＋2"结果的学术研究基础方面的作用，也是不可忽视的重要因素。所以要提倡有一个互相学习的科研集体。正因为这样，八十年代初，我们的已故导师华罗庚教授在英国访问讲学期间，英国皇家数学会的主席杜特（Todd）教授就高度评价了以华罗庚教授为首的中国数论学派的突出成就。那么，这个

学派的基本特点是什么呢？第一，华教授要求他的学生们必需具备雄厚的高等数学基础知识，要掌握较熟练的算题技能。第二，华教授要求他的学生们经常保持一个清醒的头脑，要随时明白自己的业务高度，任何时候总有自己的奋斗目标，始终有一股战斗式的业务上进心。一句话，华教授是以“严”来要求我们的，这也是我国数论研究工作作出重大成就的业务基础，没有这一点是不可思议的。因此建议，打算或正在搞哥德巴赫问题或其它著名世界难题的青年们，能正确认识这些难题的艰难性。在努力从“严”打好高初等数学基础的前提下，再来向世界难题进军！否则很可能会白费精力和时间，徒劳无功。

八 某些不定方程



在第四章中我们给出了长除法（也称辗转相除法，国外称为欧几里得算法）．利用它可以解二元一次不定方程

$$ax+by=c \tag{8.1}$$

其中a,b,c为给定的整数，$a\neq0$，$b\neq0$．

如果（8.1）有一组解x,y．那么由$(a,b)|a$以及$(a,b)|b$及(8.1)式就推出必有$(a,b)|c$．因此得到

定理 8.1 不定方程(8.1)有解的必要条件是

$$(a,b)|c.$$

现在设$(a,b)=1$，我们先来考虑如下的简单情形

$$ax+by=1 \tag{8.2}$$

由辗转相除法，一定有以下诸式成立

$$
\begin{array}{ll}
a=q_1b+r_1, & 0<r_1<b \\
b=q_2r_1+r_2, & 0<r_2<r_1 \\
\cdots\cdots & \cdots\cdots \\
r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}, & 0<r_{n-1}<r_{n-2} \\
r_{n-2}=q_nr_{n-1}+r_n, & 0<r_n<r_{n-1} \\
r_{n-1}=q_{n+1}r_n. &
\end{array}
$$

这里$r_n=(a,b)=1$，于是，从倒数第二式得到

$$1=r_n=r_{n-2}-q_nr_{n-1}$$

再将倒数第三式中$r_{n-1}=r_{n-3}-q_{n-1}r_{n-2}$代入上式得

$$
\begin{aligned}
1&=r_{n-2}-q_n(r_{n-3}-q_{n-1}r_{n-2}) \\
&=(1+q_nq_{n-1})r_{n-2}-q_nr_{n-3}
\end{aligned}
$$

依次反推过去，最后便可以得到形如

$$1=ax_0+by_0$$

的一个表达式，由此就求得(8.2)的一解x_0, y_0。而且，若 t 为任一整数，

$$x=x_0+bt,\ y=y_0-at \tag{8.3}$$

也都是(8.2)的解，这可代入(8.2)直接验证之。

下面要来证明，当x_0, y_0为(8.2)的一解时，令 t 取遍一切整数，则(8.3)就是(8.2)的全部解了。为此设$\overline{x}, \overline{y}$为(8.2)的任一解，则我们有

$$1=ax_0+by_0$$

$$1=a\overline{x}+b\overline{y}$$

两式相减得 $a(\overline{x}-x_0)=b(y_0-\overline{y})$，由于$(a,b)=1$，因此必须$a|(y_0-\overline{y})$，$b|(\overline{x}-x_0)$，于是必有 t 使 $\overline{x}-x_0=bt$，故得$b(y_0-\overline{y})=a(\overline{x}-x_0)=abt$，于是 $y_0-\overline{y}=at$，这证明了 (8.2) 的任一解必有(8.3)的形状。

当$(a,b)=d|c$时，可在(8.1)的两边用d来除，将(8.1)化为

$$Ax+By=C \tag{8.4}$$

这里 $A=a/d$，$B=b/d$，$C=c/d$，且显然有$(A,B)=1$。

我们先按上述，用辗转相除法求出

$$Ax+By=1 \tag{8.5}$$

的一组解x_0,y_0。则 $x_1=x_0C$，$y_1=y_0C$ 显然就是(8.4)的一组解。应用上面的讨论方法可证，(8.4)的全部解可以表示成

$$x=x_0C+Bt,\quad y=y_0C-At \tag{8.6}$$

其中 t 取遍一切整数。这样就获得了 (8.1) 的全部解。我们就证明了

定理 8.2 方程(8.1)有解的充分与必要条件为

$$(a,b)|c$$

下面举一个求解的例子．解方程

$$248x+124y=20 \tag{8.7}$$

解 用辗转相除法或直接分解因数可以证明284与124的最大公约数为4，即

$$(284, 124)=4$$

因为$4|20$，所以(8.7)一定可解。(8.7)两边除以4得

$$71x+31y=5 \tag{8.8}$$

我们先来求解

$$71x+31y=1 \tag{8.9}$$

由辗转相除法有

$$71=2\times 31+9 \tag{8.10}$$

$$31=3\times 9+4 \tag{8.11}$$

$$9=2\times 4+1 \tag{8.12}$$

由（8.12）式解出

$$1=9-2\times 4 \tag{8.13}$$

由（8.11）式解出$4=31-3\times 9$代入(8.13)式得

$$\begin{aligned}1&=9-2\times(31-3\times 9)\\&=7\times 9-2\times 31\end{aligned} \tag{8.14}$$

由（8.10）式解得$9=71-2\times 31$代入（8.14）式得

$$\begin{aligned}1&=7\times(71-2\times 31)-2\times 31\\&=7\times 71-16\times 31\end{aligned} \tag{8.15}$$

将(8.15)与(8.9)对照即得(8.9)的一组解为

$$x_0=7,\quad y_0=-16$$

于是(8.8)有一组解为

$$x_1=35,\ y_1=-80$$

因此(8.8)的全部解为

$$x=35+31t,\ y=-80-71t\ (t\text{为任意整数}) \tag{8.16}$$

而这也就是(8.7)的全部解.

对于多元一次不定方程,也有与定理2类似的结论成立，但求解更为复杂，这里不再赘述。对于二元二次不定方程

$$ax^2+bxy+cy^2+dx+ey+f=0 \tag{8.17}$$

它的求解问题已获得完全的解决，但是解决这个问题需要较多的数论知识，这里不能详述，下面只介绍高斯关于(8.17)的解的一个性质.

定理8.3（高斯） 如果 $D=b^2-4ac>0$，D 不是平方数，

$$\Delta=4acf+bde-ae^2-cd^2-fb^2\neq 0$$

而且(8.17)有一组整数解，那么它就有无穷多组整数解。

对于次数 $\geqslant 3$ 的多元不定方程，其解的存在性、解的个数以及如何求解都更加困难，至今仍有许多难题没有解决。

1935年，阿丁提出了一个猜测，第二年，他

猜测即被谢瓦莱证明是正确的，他们的结果的一个推论是下面的定理。

定理 8.4（阿丁—谢瓦莱） 设 $f(x_1,x_2,\cdots,x_n)$是 n 个变元的一个多元多项式，它的每一项有形状

$$cx_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$$

其中$\alpha_1,\cdots,\alpha_n$皆为非负整数，c 为常系数且$p\nmid c$，这里p为一个给定的素数。定义$\alpha_1+\cdots+\alpha_n$为这一项的次数，而 f 的所有项中最大的次数 d 就称为 f 的次数，也记为$\deg f=d$。假设

(a) $f(0,0,\cdots,0)$是 p 的倍数。

(b) $n>d$。

那么一定至少还有一组 $x_1,x_2,\cdots,x_n$，它们不全是 p 的倍数且使$f(x_1,\cdots,x_n)$仍为p的倍数。

换句话说，在所给条件下不定方程

$$f(x_1,\cdots,x_n)=py$$

至少有一组整数解 $x_1,\cdots,x_n,y$ 使 $x_1,\cdots,x_n$ 中至少有一个数不是 p 的倍数。

例如：不定方程

$$x^2+y^2+z^2=pw$$

必有适合 $p\nmid(x,y,z)$ 的整数解 x,y,z,w，这里(x,y,z)表示x,y,z这三个整数的最大公约数。

关于不定方程的可解性判别问题，希尔伯特

于1900年提出的23个著名数学问题中的第十个问题提出：设 $f(x_1,\cdots,x_n)$是一个任意给定的整系数多元多项式，试求出一个只要作有限步运算的方法来判定不定方程

$$f(x_1,\cdots,x_n)=0 \qquad (8.18)$$

是否有整数解。这个问题已经获得解决，而其答案则是否定的，即不存在这样的方法。有兴趣的读者可以参看马丁·戴维斯（M. Davis）在《美国数学月刊》（American Math. Monthly）1973年80卷第233—269页上的文章，题目是"希尔伯特第十问题是不可解的"。

但是，上面的结论只是对于一般形状的不定方程(8.18)而言说不存在有限步运算可以判别可解性的方法。而对某些特殊的方程，还是可能存在经有限步即可判别方程是否有解的方法的。本世纪六十年代后期，英国数学家爱·贝克用他的方法求出了一类不定方程整数解的具体上界值，例如他证明了

定理8.5 不定方程

$$y^2=x^3+k,\quad k\neq 0$$

的整数解 x,y 满足

$$\max(|x|,|y|)\leqslant\exp(10^{10}|k|^{10^4}) \qquad (8.19)$$

里$\max(|x|,|y|)$表示$|x|$与$|y|$中最大的数值，而$\exp(t)=e^t$。

从理论上讲，给出了解的界限(8.19)，就可以逐个用这个范围里的整数组x，y代入原方程中试算看它是否是它的解，由于(8.19)中的整数组只有有限组，故总可以在有限步运算后判定原方程是否有解，以及一共有多少组解。但由于贝克的方法给出的解的界一般仍然太大，使实际上去做很有困难。只在一些特殊情形，利用电子计算机才可以做得到。

在第五章中介绍了连分数的初步知识。利用连分数理论可以证明如下的结论。

定理8.6 如果θ是一个无理数，那么就有无穷多对整数p_n及$q_n>0$使不等式

$$\left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{q_n^2} \tag{8.20}$$

成立。

设θ是一个m次不可约整系数多项式的根，这种θ称为一个m次代数数。对于一个任给的m次代数数θ，可不可以找到无穷多组整数p_n、q_n($q_n>0$)使成立比(8.20)式更好一点的估计式

$$\left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{q_n^{2+\sigma}} \tag{8.21}$$

呢？(这里$\delta>0$是预先给定的一个随便多小的正实数）。这个问题于1958年为英国数学家罗思所解决。他给出了否定的答案，即他证明了如下的定理8.7：

定理 8.7 若θ是一个m次代数数，那么对任意预先给定的实数$\delta>0$，(8.21)只可能被有限多对整数p_n及$q_n>0$所满足。

利用定理8.7，我们可以给出一类高次不定方程的解数的一个非常有名的定理，它属于阿·由。

定理8.8 （阿·由） 设$m\geqslant 3$，$f(z)=a_m z^m+a_{m-1}z^{m-1}+\cdots+a_1 z+a_0$是一个$m$次整系数不可约多项式，那么不定方程

$$F(x,y)=a_m x^m+a_{m-1}x^{m-1}y+\cdots+a_1 xy^{m-1}+a_0 y^m=c \qquad (8.22)$$

只有有限多组整数解x,y，其中c是一个给定的整数。

这里整系数多项式不可约意义如下：设f为一个m次整系数多项式。若有两个非常数的整系数多项式f_1,f_2，使$f=f_1 f_2$，则称f为可约，反之则称f为不可约。

为了证明定理8.8，还需要若干定义和引理。

定义8.1 设 $f(z)=a_m z^m+a_{m-1}z^{m-1}+\cdots$这

$+a_1z+a_0$为一个m次多项式，称多项式

$$ma_mz^{m-1}+(m-1)a_{m-1}z^{m-2}+\cdots$$
$$+2a_2z+a_1$$

为$f(z)$的导出多项式，记为$f'(x)$。

引理8.1 如果$f(z)=0$有一个重零点，那么$f(z)$与其导出多项式$f'(z)$必有一公共零点。

（我们略去这个引理的证明）。

引理8.2 如果$f(z)$与$g(z)$为两个整系数多项式，它们有一个公共零点且$f(z)$为不可约．那么一定存在整数$M\neq0$使$f(z)$整除$Mg(z)$。

这个引理可以粗略证明于下．由$f(z)$与$g(z)$有公共零点知$f(z)$与$g(z)$必有一个非常数的公因式$d(z)$，但因为$f(z)$不可约，故$d(z)$必为$f(z)$的一个常数倍数：$d(z)=Qf(z)$，Q可能是整数，也可能是个分数．于是由$d(z)|g(z)$知，$f(z)$必整除$g(z)$的某个整倍数。

由引理8.1与引理8.2可以很容易推出下述结论。

引理8.3 如果$f(z)$为一m次整系数不可约多项式，那么$f(z)$不可能有重零点。

证明 用反证法．若$f(z)$有重零点，由引理8.1知$f(z)$与其导出多项式$f'(z)$必有一个公共零点，但$f(z)$不可约，于是再由引理8.2有整数$M\neq0$

使$f(z)$整除$Mf'(z)$，但f'的次数为$m-1$，而$f(z)$次数为m，因此这是不可能的。

下面可以来证明定理8.8了。

首先考虑 $c=0$ 的简单情形。我们来证明$F(x,y)=0$ 只有一组零解$x=y=0$。

首先若$y=0$，由$F(x,y)=0$就得必有$x=0$。再设$F(x,y)=0$有一组解 $x_0\neq0$，$y_0\neq0$。那么显然x_0/y_0就是$f(z)$的一个根。于是一定存在一个$m-1$次有理系数多项式$g(z)$使

$$f(z)=(z-x_0/y_0)g(z) \tag{8.23}$$

这里不妨假定$f(z)$的诸系数之最大公因数为1。

既然$g(z)$是有理系数多项式，取M为其诸系数分母的最小公倍数易见$Mg(z)$就是一个整系数多项式了，记

$$Mg(z)=b_{m-1}z^{m-1}+\cdots+b_1z+b_0$$

就有

$$My_0f(z)=(y_0z-x_0)(b_{m-1}z^{m-1}+\cdots+b_1z+b_0) \tag{8.24}$$

用$d_1=(y_0,x_0)$表示y_0与x_0之最大公因数，用 $d_2=(b_{m-1},\cdots,b_1,b_0)$表示$Mg(z)$的系数$b_{m-1},\cdots,b_1$，$b_0$之最大公因数。我们要证明有

$$My_0=d_1d_2 \tag{8.25}$$

我们不妨设 $d_1=d_2=1$ 来证 $My_0=1$ 即可。如果

不然，就要有至少一个素数 $p|My_0$。但由于 $d_1=1$，于是必$p\nmid y_0$或$p\nmid x_0$，不妨只讨论$p\nmid x_0$的情形。又由$d_2=1$知必有一个指标 r 使

$$p|b_{n-1},\cdots,p|b_{r+1},p\nmid b_r$$

我们来考虑 $My_0f(z)$ 的展式中 z^r 项的系数，由(8.24)式知这系数等于

$$-x_0b_r+y_0b_{r-1}$$

如果$p|y_0$，那么$p|(y_0b_{r-1})$，但 $p\nmid(x_0b_r)$，故 p 不能整除$My_0f(z)$ 中 z^r 项系数，这与 $p|My_0$ 矛盾。如果$p\nmid y_0$且$p\nmid x_0$，可以改为考虑$M\ y_0f(z)$中 z^{r+1}项系数

$$-x_0b_{r+1}+y_0b_r$$

由 $p|b_{r+1}$ 及 $p\nmid(y_0b_r)$知，p 也不能整除这个系数，这仍与$p|My_0$的假设矛盾，故只可能

$$My_0=1$$

这就证明了(8.25)式。取整数

$$N=\frac{M}{d_2}=\frac{d_1}{y_0}$$

（因$d_2|M$，故M/d_2为整数，由(8.25)式知 $d_1/y_0=M/d_2$也必为整数），我们就有

$$f(z)=\frac{1}{N}\left(z-\frac{x_0}{y_0}\right)\cdot Ng(z) \qquad (8.26)$$

这里

$$\frac{1}{N}\left(z-\frac{x_0}{y_0}\right)=\frac{y_0}{d_1}\left(z-\frac{x_0}{y_0}\right)$$

$$= \frac{1}{d_1}(y_0 z - x_0)$$

与 $$Ng(z) = \frac{M}{d_2} g(z)$$

皆为整系数多项式。但(8.26)式显然与$f(z)$不可约的假定矛盾。因此$F(x,y)=0$只可能有一组解$x=y=0$。

现在讨论$c\neq 0$的情形。

由代数基本定理，$f(z)$有m个复根$\theta_1,\cdots,\theta_m$，故有

$$F(x,y) = a_m(x-\theta_1 y)\cdots(x-\theta_m y) = c \tag{8.27}$$

我们先来证(8.22)只有有限多组整数解x，$y(y>0)$。对每一组这种解，皆有(8.27)式成立。于是

$$|a_n||x-\theta_1 y|\cdots|x-\theta_m y| = |c|,$$
$$y>0 \tag{8.28}$$

取 $|x-\theta_1 y|,\cdots,|x-\theta_m y|$ 中最小的一个记为$|x-\theta_k y|$，则

$$|a_n||x-\theta_k y|^m \leqslant |a_n||x-\theta_1 y|\cdots |x-\theta_m y| = |c|$$

故

$$|x-\theta_k y| \leqslant \alpha \tag{8.29}$$

这里$\alpha>0$且$\alpha^m = |c|/|a_n|$。

由于$f(z)$不可约，由引理8.3知$f(z)$的根θ_1，

$\cdots,\theta_m$两两不同。故对任一对根$\theta_k,\theta_l,k\neq l$，皆有一个常数$\beta$存在使

$$|\theta_k-\theta_l|\geqslant\beta>0 \tag{8.30}$$

我们有

$$\begin{aligned}|x-\theta_l y| &= |(\theta_k-\theta_l)y+(x-\theta_k y)|\\ &\geqslant \beta y-\alpha,\ (l\neq k)\end{aligned} \tag{8.31}$$

如果(8.22)有无穷多组整数解$x,y(y>0)$，那么就有无穷多个解$x,y(y>0)$适合$y>2\frac{\alpha}{\beta}$。对这无穷组解，由(8.31)式得到有

$$|x-\theta_l y|\geqslant\beta y-\alpha>\frac{1}{2}\beta y,\ \ l\neq k \tag{8.32}$$

于是将(8.32)式代入(8.28)式即得到

$$|a_n|\left(\frac{1}{2}\beta y\right)^{m-1}|x-\theta_k y|$$

$$<|a_n||x-\theta_1 y|\cdots|x-\theta_m y|=|c|$$

此即有无穷多对整数$x,y\left(y>2\frac{\alpha}{\beta}\right)$使

$$|x-\theta_k y|<\left(\frac{2^{m-1}|c|}{|a_n|\beta^{m-1}}\right)\frac{1}{y^{m-1}}$$

成立，即使

$$\left|\theta_k-\frac{x}{y}\right|<\frac{A}{y^m}$$

成立，这里 $A=\frac{2^{m-1}|c|}{|a_n|\beta^{m-1}}>0$。当$y>A^2$ 时这种x,y仍有无穷对，它们使

$$\left|\theta_k-\frac{x}{y}\right|<\frac{1}{y^{m-\frac{1}{2}}}$$

成立，而这与定理8.7矛盾(注意$m\geqslant3$的条件)。

剩下还要证明，(8.22)的满足$y<0$的解 x,y也只可能有有限多组，这只要考虑 $F(x,-y)=c$就行了，这点留给读者作为练习。最后当$c\neq0$而$y=0$时(8.22)显然也只有有限组整数解。这就完成了定理8.8之证明。

最后我们来介绍一下不定方程中一个最引人注意的问题—费马大定理。这个结论说的是：对$n\geqslant3$，不定方程

$$x^n+y^n=z^n \tag{8.33}$$

没有适合$xyz\neq0$的整数解。

首先容易证明，如果

$$x^4+y^4=z^4 \tag{8.34}$$

与

$$x^p+y^p=z^p \text{ （}p\text{ 为奇素数）} \tag{8.35}$$

均无适合 $xyz\neq0$ 的整数解，那么(8.33)一定无适合$xyz\neq0$的整数解。

这是因为任给一整数 $n\geqslant3$，要么$4|n$，要么有一个奇素数$p|n$。在每一种情形，由(8.34)与

(8.35)无适合$xyz\neq0$的整数解即知(8.33)必无适合 $xyz\neq0$ 的整数解。下面来证 (8.34)无适合 $xyz\neq0$ 之整数解。容易看出只需证出下述结论即可。

定理8.9 不定方程

$$x^4+y^4=z^2 \tag{8.36}$$

没有适合$xyz\neq0$的整数解。

证明 我们只需证明(8.36)没有适合$(x,y,z)=1$且$z>0$的非零整数解即可。这点留给读者去验证（这里(x,y,z)表示x,y,z之最大公因数）。

用反证法，设(8.36)有一组解适合$(x,y,z)=1$，$xyz\neq0$ 且 $z>0$。那么x与y不可能全为奇数。否则的话，设$x^2=2m+1$，$y^2=2n+1$，则有

$$x^4=4(m+1)m+1,\quad y^4=4(n+1)n+1$$

于是

$$x^4+y^4=4(m(m+1)+n(n+1))+2$$

即x^4+y^4被4除余数为2。而当$2|z$时有$4|z^2$，$2\nmid z$时有$z=2l+1$，故$z^2=4(l+1)l+1$，于是z^2被4除余数或为0或为1，不可能为2。因而x与y不可能同为奇数。假设x为奇数，y为偶数，于是z为奇数。我们有

$$y^4=(z-x^2)(z+x^2) \tag{8.37}$$

如果有一个素数p既整除$z-x^2$，又整除$z+$

x^2，那么必$p|(z-x^2)+(z+x^2)=2z$，且$p|(z+x^2)-(z-x)^2=2x^2$。如果$p\neq 2$，那么$p|z$，$p|x$，由（8.37）式又有$p|y$。这与$(x,y,z)=1$矛盾。因此只可能$p=2$，又由x与z皆为奇数知确有$2|(z+x^2)$，$2|(z-x^2)$，因此证得$z+x^2$与$-x^2$之最大公因数恰为2，即

$$(z+x^2,z-x^2)=2 \qquad (8.38)$$

由(8.37)知$z-x^2$与$z+x^2$之积是一个四次方，于是只有以下两种可能性成立。

情形一　$z-x^2=2a^4$，$a>0$，$2\nmid a$，

$z+x^2=8b^4$，$(a,b)=1$。

情形二　$z-x^2=8b^4$，

$z+x^2=2a^4$，$a>0$，$2\nmid a$，$(a,b)=1$。

由情形一推出

$$2x^2=(z+x^2)-(z-x^2)=8b^4-2a^4$$

即

$$x^2=4b^2-a^4 \qquad (8.39)$$

但(8.39)式不可能成立。因$2\nmid x$，故x^2被4除余1，而a^2为奇数，故$a^4=(a^2)^2$被4除余1，所以$4b^2-a^4$被4除余-1，故(8.39)不可能成立。于是只可能情形二成立，由此推出

$$z=4b^4+a^4 \qquad (8.40)$$

由此顺便看出$1\leqslant a<z$。在情形二中消去z得到

$$x^2=a^4-4b^4$$

故有

$$4b^4=(a^2-x)(a^2+x) \qquad (8.41)$$

由$(a,b)=1$知必有$(a,x)=1$，因为若有$d>1$使$(a,x)=d$，由(8.41)就有$d|4b^4$，若$d|b$，就与$(a,b)=1$矛盾。若$2|d$，就有$2|x$，这与$2\nmid x$矛盾。这就证明了$(a,x)=1$。于是与上面证法相同可以推出有$(a^2-x,a^2+x)=2$，由(8.41)知必有$a^2-x=2x_1^4$，$a^2+x=2y_1^4$，相加得到

$$a^2=x_1^4+y_1^4$$

于是又得到(8.36)的一组解x_1,y_1,a，其中$(a,x_1,y_1)=1$且$0<a<z$。

这样就可以无限做下去得到(8.36)的解x_r,y_r,z_r，其中$(x_r,y_r,z_r)=1$，$z>z_r>0$，这是不可能的，因为不超过z的正整数只有有限多个。定理8.9证毕。 □

证明定理8.9的这个方法称为“无穷递降法”，它属于费马。费马创造的这一方法不但可以用来证明某种方程无解，也可以从某种方程有一组解而造出它的无穷组解。下面以马尔科夫方程

$$x^2+y^2+z^2=3xyz \qquad (8.42)$$

为例说明之。

显然，$x=y=z=1$为(8.42)的一组正整数解，

我们要证明(8.42)有无穷多组正整数解，且这些解都可以从$x=y=z=1$这组解生出来。

设x_0,y_0,z_0为(8.42)的一组解，则由

$$\begin{aligned}&x_0^2+y_0^2+(3x_0y_0-z_0)^2\\&=x_0^2+y_0^2+z_0^2+9x_0^2y_0^2-6x_0y_0z_0\\&=3x_0y_0z_0+9x_0^2y_0^2-6x_0y_0z_0\\&=3x_0y_0(3x_0y_0-z_0)\end{aligned}$$

知，$x_0,y_0,3x_0y_0-z_0$也是(8.42)的一组解.下面要来证明，(8.42)的任一组正整数解皆可从$x=y=z=1$这组解出发用上法造出来。

设x,y,z为(8.42)的一组正整数解，$xyz\neq1$。

先讨论$x=y$，但$z\neq x$的情况。此时(8.42)变为

$$2x^2+z^2=3x^2z \tag{8.43}$$

于是有$x^2|z^2$，从而$x|z$。令$z=xw$得到

$$2x^2+(xw)^2=3x^2(xw)$$

消去x^2得

$$2+w^2=3xw\quad(w>0) \tag{8.44}$$

于是$w|(3xw-w^2)=2$。即$w=1$或$w=2$。若$w=1$，就有$z=xw=x$，这不可能.故只可能$w=2$，代入(8.44)得$x=1$，于是$y=x=1$，$z=xw=2$。显然$x=y=1$，$z=2$这组解可从$x_0=y_0=z_0=1$这

组解用公式

$$x=x_0=1,\ y=y_0=1,\ z=3x_0y_0-z_0=2$$

造出来。

下面讨论$1\leqslant x<y<z$成立的情形。我们首先证明$3xy-z<z$。

由 $z^2-3xyz+(x^2+y^2)=0$

可解得 $2z=3xy\pm\sqrt{9x^2y^2-4(x^2+y^2)}$

$$(8.45)$$

若(8.45)式中负号成立，则由

$$8x^2y^2-4(x^2+y^2)$$
$$=4x^2(y^2-1)+4y^2(x^2-1)>0$$

知道

$$\sqrt{9x^2y^2-4(x^2+y^2)}$$
$$=\sqrt{x^2y^2+8x^2y^2-4(x^2+y^2)}>\sqrt{x^2y^2}=xy$$

于是就有

$$2z<3xy-xy=2xy$$

即

$$z<xy \qquad (8.46)$$

于是就有

$$3xyz=x^2+y^2+z^2<3z^2 \text{（因}x<y<z\text{）}$$

由此推得

$$xy<z \qquad (8.47)$$

这与(8.46)式矛盾，故不可能。

故只可能(8.45)式中正号成立：

$$2z=3xy+\sqrt{9x^2y^2-4(x^2+y^2)}$$

于是有 $2z>3xy$，即 $3xy-z<z$。

这就表明从适合$1\leqslant x<y<z$的这组解出发造出的新解 $x_1=x, y_1=y, z_1=(3xy-z)$ 满足条件 $x_1+y_1+z_1<x+y+z$。如果x_1, y_1, z_1中已有两个数相等，这就化为已证过的情形。若不然，适当安排次序仍可假设有

$$1\leqslant x_1<y_1<z_1$$

对它再用上法造出新解$x_2=x_1, y_2=y_1, z_2=3x_1y_1-z_1$，则必有$x_2+y_2+z_2<x_1+y_1+z_1$，由于$x+y+z$ 是有限的，经上法有限步后必可化为已证过的x, y, z 中至少有二数相等的情况。这种解已证得必可从$x=y=z=1$用所述方法造出来。这就证明了：方程(8.42)有无穷多个正整数解，且这些解皆可由所述方法造出来。

对于方程(8.35)，可以变形为

$$x^p+y^p+z^p=0(p\text{为奇素数}) \quad (8.48)$$

1823年斯·吉门用完全初等的方法证明了

定理8.10 若p为奇素数且 $q=2p+1$ 仍为素数，则(8.48)没有满足 $p\nmid xyz$ 的整数解。

这个定理的证明要用到本书范围外的一些初

等数论知识，故不能在此给出。

1850年库默尔创造了理想数这一概念，并用之于解决费马大定理，获得了重要的进展。为了叙述他的这一结果，先给出如下几个定义。

定义8.2 定义$B_0=1$，在$B_1,\cdots,B_{m-1}$已知时，B_m由下式归纳地定义之：

$$(m+1)B_m=-\sum_{k=0}^{m-1}\binom{m+1}{k}B_k \quad (8.49)$$

诸数$B_0,B_1,\cdots$称为伯努利数。

容易证明，除$B_1=-\frac{1}{2}\neq 0$外，一切$B_{2l+1}=0(l\geqslant 1)$，又所有B_m皆为有理分数。

定义8.3 设p为一奇素数且它不整除$B_2,B_4,\cdots,B_{p-3}$的任一分数之分子，则称p为一个正则素数。

例如在100以内只有37、59及67这三个非正则素数。现在只知道有无穷多个非正则素数，而并不知道是否有无穷多个正则素数存在。

下面可以叙述库默尔的著名结果了。

定理8.11 若p为一正则素数，那么

$$x^p+y^p=z^p$$

无正整数解。

1983年，一位西德年仅29岁的数学家法尔丁

斯应用代数几何的方法证明了莫台尔1922年提出的一个猜想，由此他就证得了下述重要结果。

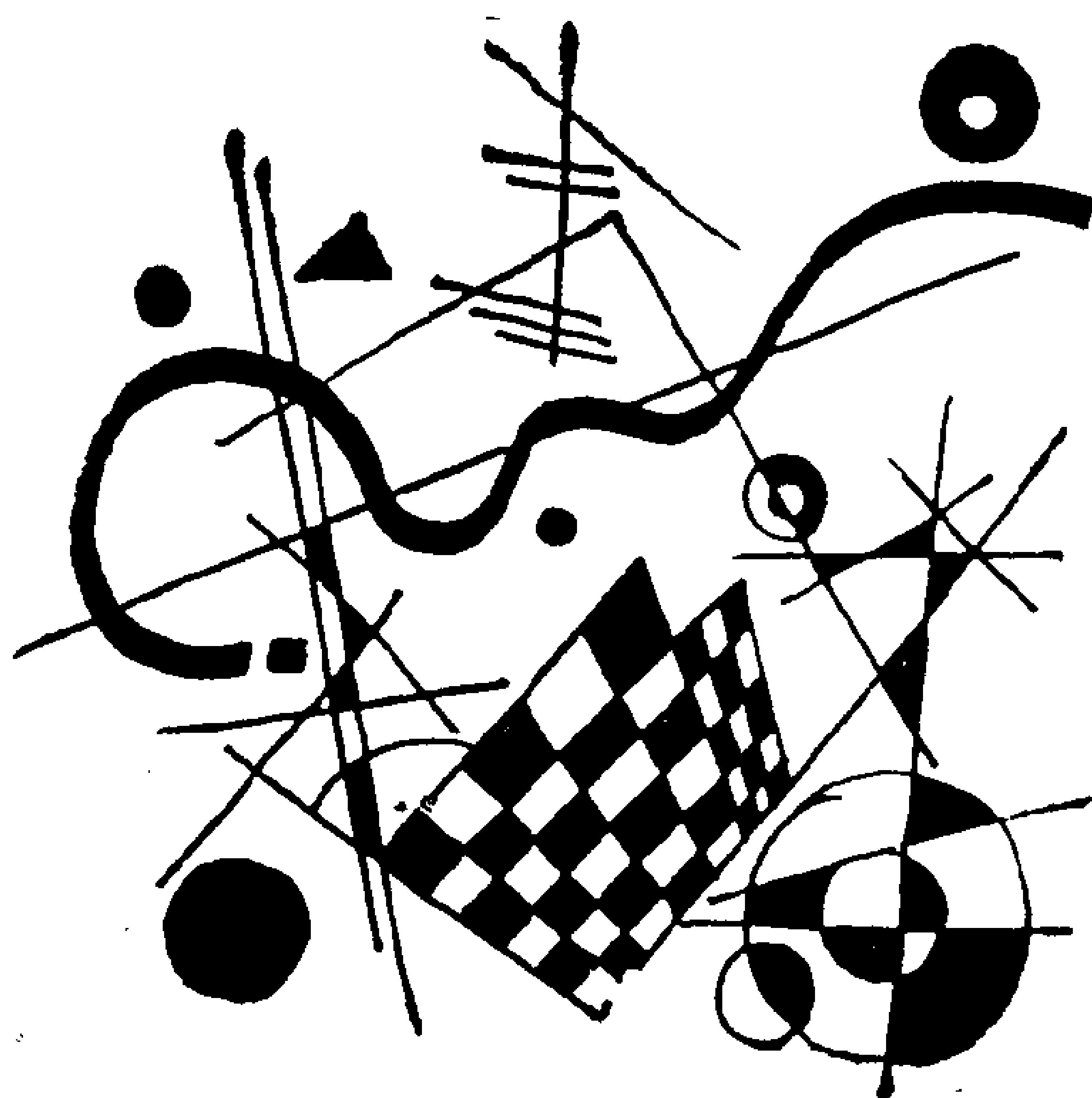
定理8.12 对每个素数$p\geqslant 3$，方程

$$x^p+y^p=z^p$$

至多只能有有限组正整数解。

但是，这些结果离完全解决费马大定理仍相差甚远。

九 若干恒等式



数论中有许多重要定理的证明与某种恒等式有密切的关系。因此，善于发现并成功地应用各种恒等式来帮助解决数论乃至其他数学分支中的一些问题，是数学家们经常使用的一种技巧。从一些看起来非常简单的恒等式出发，甚至可以建立起一套崭新的数学方法。在这一章里，我们要向大家介绍若干有趣的恒等式。

定理9.1 设a_i与b_i($i=1,2,3,4$)皆为任意复数，那么有以下二式成立：

$$(a_1^2+a_2^2)(b_1^2+b_2^2)$$
$$=(a_1b_1+a_2b_2)^2+(a_1b_2-a_2b_1)^2 \quad (9.1)$$

$$(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)$$
$$=(a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2$$
$$+(a_1b_2-a_2b_1-a_3b_4+a_4b_3)^2$$
$$+(a_1b_3+a_2b_4-a_3b_1-a_4b_2)^2+(a_1b_4$$

$$-a_2b_3+a_3b_2-a_4b_1)^2 \qquad (9.2)$$

证明 (9.1)式容易直接验证。

(9.2)式也可以直接验证，也可以利用(9.1)式证明如下。

$$\begin{aligned}
&(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)\\
&=(a_1^2+a_2^2)(b_1^2+b_2^2)\\
&\quad+(a_1^2+a_2^2)(b_3^2+b_4^2)\\
&\quad+(a_3^2+a_4^2)(b_1^2+b_2^2)\\
&\quad+(a_3^2+a_4^2)\ b_3^2+b_4^2)\\
&=(a_1b_1+a_2b_2)^2+(a_1b_2-a_2b_1)^2\\
&\quad+(a_1b_3+a_2b_4)^2+(a_1b_4-a_2b_3)^2\\
&\quad+(a_3b_1+a_4b_2)^2+(a_3b_2-a_4b_1)^2\\
&\quad+(a_3b_3+a_4b_4)^2+(a_3b_4-a_4b_3)^2 \qquad (9.3)
\end{aligned}$$

我们有

$$\begin{aligned}
&(a_1b_1+a_2b_2)^2+(a_3b_3+a_4b_4)^2\\
&=(a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2\\
&\quad-2(a_1b_1+a_2b_2)(a_3b_3+a_4b_4) \qquad (9.4)
\end{aligned}$$

$$\begin{aligned}
&(a_1b_2-a_2b_1)^2+(a_3b_4-a_4b_3)^2\\
&=(a_1b_2-a_2b_1-a_3b_4+a_4b_3)^2\\
&\quad+2(a_1b_2-a_2b_1)(a_3b_4-a_4b_3) \qquad (9.5)
\end{aligned}$$

$$\begin{aligned}
&(a_1b_3+a_2b_4)^2+(a_3b_1+a_4b_2)^2\\
&=(a_1b_3+a_2b_4-a_3b_1-a_4b_2)^2\\
&\quad+2(a_1b_3+a_2b_4)(a_3b_1+a_4b_2) \qquad (9.6)
\end{aligned}$$

$$(a_1b_4-a_2b_3)^2+(a_3b_2-a_4b_1)^2$$
$$=(a_1b_4-a_2b_3+a_3b_2-a_4b_1)^2$$
$$-2(a_1b_4-a_2b_3)(a_3b_2-a_4b_1) \quad (9.7)$$

容易验证

$$-2(a_1b_1+a_2b_2)(a_3b_3+a_4b_4)$$
$$+2(a_1b_2-a_2b_1)(a_3b_4-a_4b_3)$$
$$+2(a_1b_3+a_2b_4)(a_3b_1+a_4b_2)$$
$$-2(a_1b_4-a_2b_3)(a_3b_2-a_4b_1)$$
$$=0 \quad (9.8)$$

于是由(9.3)—(9.8)式就证得(9.2)的结论。

在初等数论中有一条著名的定理：如果 p 是一个形如$4k+1$ 的素数，那么 p 必可以表示成为两个正数的平方和。

例如：$5=1^2+2^2$，$13=2^2+3^2$，$17=1^2+4^2$，$29^2=2^2+5^2$，$37=1^2+6^2$，…等等。其中5，13，17，29，37皆为被 4 除余 1 的素数，也即皆有$4k+1$之形状。

由此定理并利用定理9.1的（9.1）式立即推出，任何两个形如$4k+1$的素数之积仍可表为两个整数的平方和。应用数学归纳法不难证明：设p_1，p_2，…，p_s是 s 个形如$4k+1$之素数（它们中可以有相重的出现），那么$p_1p_2\cdots p_s$必可表示为两个整数的平方和。这点留给读者做为一个练习。

任意给定一个自然数$n>1$。由算术基本定理知道，n必可以唯一地分解成素数之乘积：

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$$

其中p_1，…，p_s皆为互不相同之素数，$\alpha_1\geqslant 1$，…，$\alpha_s\geqslant 1$。

如果p_1，p_2，…，p_s皆为形如$4k+1$之素数，那么由上述即知n可以表示为二整数之平方和。

如果$p_1=2$，那么由$2=1^2+1^2$以及上面的讨论知，当n的素因数除2以外都形如$4k+1$时，这种自然数n必仍可表示为二整数之平方和。

如果有一个素因数（比方说p_1）是形如$4k+3$的，结论一般就不再成立了。因为任何一个形如$4k+3$的素数p不可能表为二整数之平方和，这可以证明如下：用反证法，设$p=a^2+b^2$。若$x=2l$为一个偶数，易见$x^2=4l^2$被4除余数为0，若$x=2l+1$为一个奇数，易见$x^2=4(l+1)l+1$被4除余数为1.因而a^2与b^2被4除的余数只有0与1两种可能，因此a^2+b^2被4除，余数只可能为0，1及2这三者之一，但p已知被4除余3，故不可能！

既然形如$4k+3$的素数一定不能表示成为二正数之平方和，那么上面的一切讨论就不能成立了，也就是当n含有形如$4k+3$的素因子时它一

般不再能表为二整数之平方和了。但是如果 p 是形如$4k+3$之素数， $p^{2a}|n$， $p^{2a+1}\nmid n$($a\geqslant 1$ 为整数)，那么$n=((p^a)^2+0^2)n_1$，只要n_1可以表为二平方数之和，由定理9.1的(9.1)式立即得知n也可表为二平方数之和.这样我们就证明了以下的结论。

定理9.2 设 $n>1$ 为整数，如果它有一个形如$4k+3$的素因数 p，就必有整数$a\geqslant 1$使$p^{2a}|n$，而$p^{2a+1}\nmid n$。那么 n 一定可以表示成为两个整数的平方和。

附带说一下，定理9.2中的条件还是必要的，但是它的证明超出了这本小册子的范围，不能在此给出。

我们已经证明了形如 $4k+3$之素数必不能表为二平方数之和，那么，这种素数可用几个平方数之和表示出来呢？让我们先看几个例子：

$7=1^2+2^2+1^2+2^2$，即7可以表为四个整数之平方和。而且很容易验证，7不能用三个整数之平方和表示。

$11=1^2+1^2+3^2$.即11可以表为三个整数之平方和。

$19=1^2+3^2+3^2=1^2+1^2+1^2+4^2$，即19可以表为四个整数之平方和，也可以表为三个整数之平方和。

由以上的例子很自然导出如下的猜想：每个形如$4k+3$之素数可以表示成四个整数之平方和。这个猜想是对的，由它和关于形如$4k+1$之素数可表为二整数平方和这个结果合起来，就有以下的定理成立。

定理9.3 每个素数都可以表为四个整数的平方之和。

这个定理的证明也超出了本书范围，故不能在此详述。

设p与q为任何两个素数，由定理9.3知必有整数a_1, a_2, a_3, a_4及b_1, b_2, b_3, b_4使

$$p = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

$$q = b_1^2 + b_2^2 + b_3^2 + b_4^2$$

代入定理9.1的(9.2)式知pq仍然可以表为四个整数的平方和。

$$pq = A^2 + B^2 + C^2 + D^2$$

这里可取

$$A = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4$$

$$B = a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3$$

$$C = a_1b_3 + a_2b_4 - a_3b_1 - a_4b_2$$

$$D = a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1$$

应用数学归纳法不难证明，任意有限多个素数的乘积仍然可表为四个整数的平方之和。由算术基

本定理，每个整数$n>1$皆可表为有限多个素数的乘积，这样，我们就利用定理9.3以及定理9.1的（9.2）式证明了如下著名的拉格朗日的四平方定理.

定理9.4（拉格朗日） 每个整数 $n\geqslant 1$皆可表为四个整数的平方和.

下面来讨论其它的恒等式.1770年，德国数学家华林提出一个猜想：凡正整数必可表为四个平方数之和，九个立方数之和，十九个四方数之和等等.精确地说，华林猜测对任给的正整数$k\geqslant 2$，都存在一个正整数$S(k)$，使任一正整数n皆可表为$S(k)$个非负整数的k次方之和：

$$n=a_1^k+\cdots+a_s^k\quad(\text{一切}a_i\geqslant 0)$$

令$g(k)$为使上式对一切$n\geqslant 1$有解的$S(k)$中最小的正整数，华林猜想有$g(2)=4$，$g(3)=9$，$g(4)=19$，$g(5)=37$，…等等. 其中$g(2)=4$就是定理9.4，这个著名的华林问题今天已基本上得到解决，但它的解需要用到复杂高深的解析数论方法，不能在这里介绍. 下面要介绍另一个恒等式，利用它可以给出$g(4)$的一个上界估计值.

定理9.5 设a,b,c,d为任意整数，则

$$6(a^2+b^2+c^2+d^2)^2$$
$$=(a+b)^4+(a-b)^4+(c+d)^4$$

$$+(c-d)^4+(a+c)^4+(a-c)^4$$
$$+(b+d)^4+(b-d)^4+(a+d)^4+(a-d)^4$$
$$+(b+c)^4+(b-c)^4 \qquad (9.9)$$

请读者自己验证这个恒等式的正确性.

任给一个正整数 n，它被 6 除余数只有 0，1,2,3,4,5这几种可能，于是总有整数$N\geqslant 0$使

$$n=6N+r,\quad r=0,1,2,3,4,5$$

由定理9.4有非负整数A,B,C,D使

$$N=A^2+B^2+C^2+D^2 \qquad (9.10)$$

再由定理9.4，有非负整数a,b,c,d使

$$A=a^2+b^2+c^2+d^2 \qquad (9.11)$$

于是

$$6A^2=6(a^2+b^2+c^2+d^2)^2 \qquad (9.12)$$

利用定理9.5立即推出，$6A^2$可以表为12个整数的四次方之和. 对$6B^2,6C^2$及$6D^2$运用同样的方法易得，它们都可以表为12个整数的四次方之和，于是$6N$可以表为$12\times 4=48$ 个整数的四次方之和. 最后，注意到

$$0=0^4$$
$$1=1^4$$
$$2=1^4+1^4$$
$$3=1^4+1^4+1^4$$
$$4=1^4+1^4+1^4+1^4$$

$$5=1^4+1^4+1^4+1^4+1^4$$

我们就证明了：每个正整数皆可表为至多48＋5＝53个整数的四次方之和，也就是$g(4)\leqslant 53$。如果分析得更细一点，53还可以改进得更小一些，另外这种类型的恒等式还有许多，它们在用初等方法求$g(k)$的上界时有重要的应用，这里就不一一介绍了。

下面要讨论另一类有趣的恒等式。为此先介绍几个有关的定义。

定义9.1* 设α为一个实数，记号〔α〕表示不超过α的最大整数。例如：〔0〕＝0，〔2〕＝2，〔－1〕＝－1，[4.9]＝4，[－7.1]＝－8。

定义9.2 设$g(x)$为一个对$x\geqslant 0$有定义的函数，记号$\sum\limits_{x=1}^{n}g(x)$定义为$g(1)+g(2)+\cdots+g(n)$。

以下我们讨论对$x\geqslant 0$有定义的函数$y=f(x)$，并用$f^{-1}(x)$记它的反函数，且设$f(x)$满足以下两个条件：

(ⅰ)单调增加：对$0\leqslant x_1<x_2$有$f(x_1)<f(x_2)$。

(ⅱ)$0<f(1)\leqslant 1$。

---

* 这个定义在第五及六章中均已讲过，此处仅作再次重申。

这里有两点需要说明．第一，对任给的一个函数，其反函数不一定存在，例如：$y=1$，由于$y=1$时有无穷多个x值与之对应，因而反函数不存在；再如$y=x^2$，对$y=a>0$，有$\pm\sqrt{a}$两个x值与之对应，因而其反函数也不存在（如果定义域为x可取一切实数的话），但若限制$y=x^2$只在$x>0$有定义，那么对每个$y=a\geqslant0$，恰有一个$x=+\sqrt{a}$与之对应，这时$y=x^2$就有反函数$x=+\sqrt{y}$存在。特别地可以证明：若$y=f(x)$是x的严格单调函数，则它必有反函数存在，且反函数也是严格单调的（注：设$y=f(x)$在$x\geqslant0$定义且对任二点$x_1<x_2$有$f(x_1)\leqslant f(x_2)$，就称f是单调增加的函数，若对$x_1<x_2$有严格不等式$f(x_1)<f(x_2)$成立，则称f为严格增加的函数，限制条件(i)就是为了保证f有反函数存在。当然，若f有反函数存在，f不一定非是单调函数不可）．第二，限制条件(ii)其实不是个严重的限制，因为如果$f(x)$严格单调，但不满足(ii)，比方有实数$t>1$使得$t<f(1)\leqslant t+1$那么只要改为考虑函数$F(x)=f(x)-t$就行了，因为此时$F(x)$一定已经满足(i)(ii)两个条件．我们要来证明下面的恒等式．

定理9.6 设$f(x)$满足条件(ⅰ)、(ⅱ),则对任何正整数n及$m=[f(n)]$,有

$$\sum_{j=1}^{n}[f(j)]+\sum_{k=1}^{m}[f^{-1}(k)]=nm+d$$

这里f^{-1}为f之反函数,d为$j=1,\cdots,n$这n个数中使$f(j)$为整数的j的个数。

证明 绘出$y=f(x)$在$\frac{1}{2}\leqslant x\leqslant n$之间的图形(见图9.1),由直线

$$x=\frac{1}{2},\quad x=n,\quad y=f\left(\frac{1}{2}\right),\ y=f(n)$$

围成一个矩形,记为$ABCD$。曲线将此矩形分成

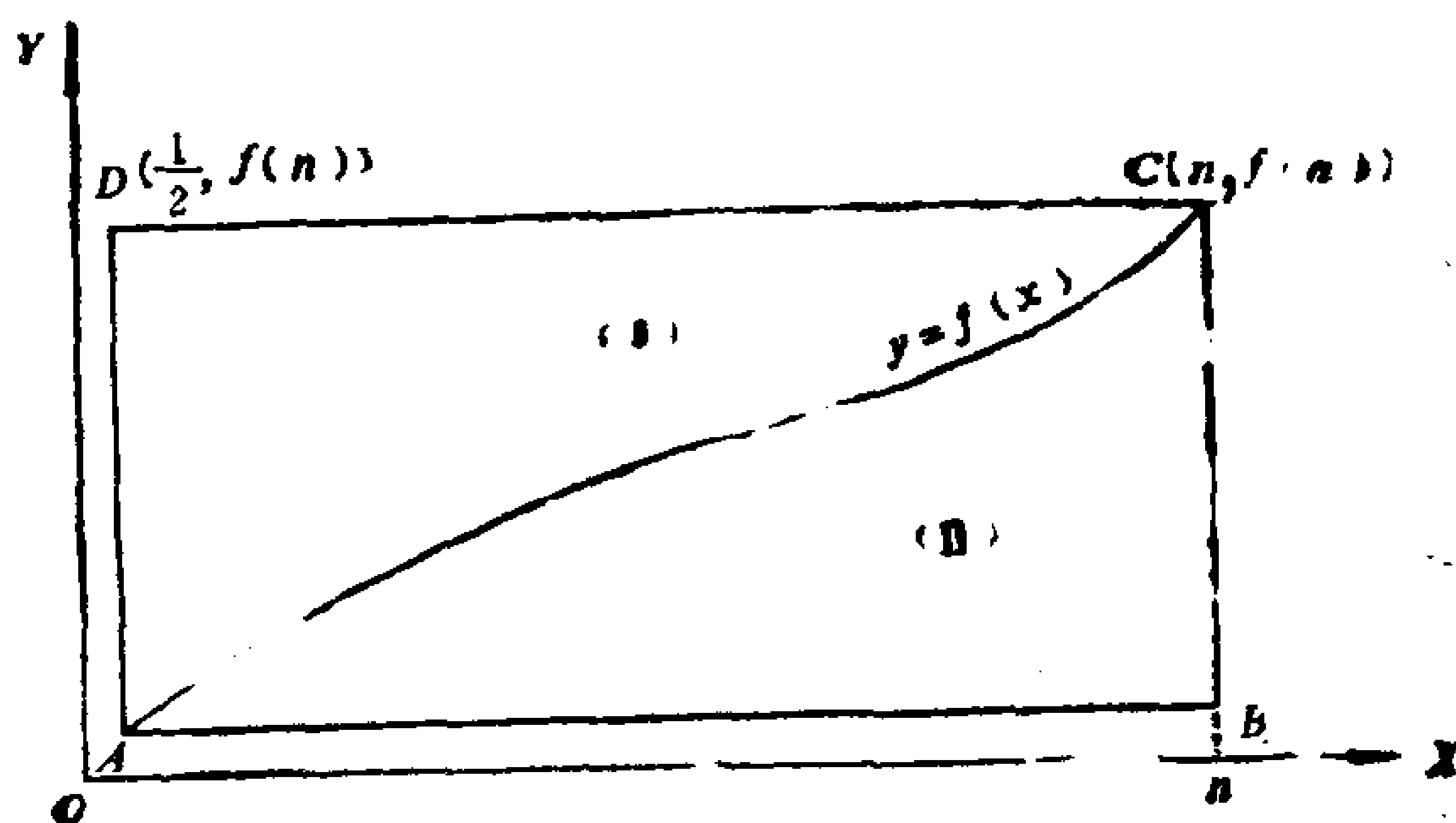


图 9.1

上下两部分,分别记为(Ⅰ)与(Ⅱ).在这个xoy坐标系中,每个点都有两个坐标:横坐标x及纵坐标

y，如果x与y这两个数恰好都是整数，我们就称这点为一个整点（或格点）。容易看出，和$\sum_{j=1}^{n}[f(j)]$恰好表示区域（Ⅱ）的内部以及其边界线上全部整点的个数。而$\sum_{k=1}^{m}[f^{-1}(k)]$恰为区域（Ⅰ）的内部及其边界线上整点的个数。因此$\sum_{j=1}^{n}[f(j)]+\sum_{k=1}^{m}[f^{-1}(k)]$就是矩形内部和四边上的所有整点个数加上在曲线段$y=f(x)$，$\frac{1}{2}\leqslant x\leqslant n$上的整点个数。而矩形$ABCD$内部及四边上整点个数恰为$nm$，曲线段$y=f(x)$，$\frac{1}{2}\leqslant x\leqslant n$上整点个数恰为$d$，合起来就证明了我们的结论。

下面来给出几个应用的例子。

例9.1　取$f(x)=\sqrt{x}$，则易见反函数为$f^{-1}(x)=x^2$。取$m=[\sqrt{n}]$，由定理 9.6 得到恒等式

$$\sum_{j=1}^{n}[\sqrt{j}]+\sum_{k=1}^{[\sqrt{n}]}k^2=nm+m=(n+1)[\sqrt{n}] \tag{9.13}$$

这是因为$\sqrt{x}$仅当x为平方数时才取整数值，因而恰有$d=m$。

由于

$$\sum_{k=1}^{[\sqrt{n}]} k^2 = \frac{1}{6}[\sqrt{n}]([\sqrt{n}]+1)(2[\sqrt{n}]+1) \tag{9.14}$$

将(9.14)代入(9.13)式中得到

$$\sum_{j=1}^{n}[\sqrt{j}] = (n+1)[\sqrt{n}] - \frac{1}{6}[\sqrt{n}]([\sqrt{n}]+1)(2[\sqrt{n}]+1) \tag{9.15}$$

例9.2　设a，b为两个互素之正整数，$a<b$，而$f(x)=ax/b$，则取$m=[an/b]$，由定理9.6得到

$$\sum_{j=1}^{n}[aj/b] + \sum_{k=1}^{m}[bk/a] = nm + \left[\frac{n}{b}\right] \tag{9.16}$$

特别地，若a与b还是奇数，取$n=\frac{1}{2}(b-1)$，我们来确定$m=[an/b]=\left[\frac{a(b-1)}{2b}\right]$的值。

首先易见有

$$\frac{a(b-1)}{2b} < \frac{a}{2} \tag{9.17}$$

又由$a<b$有$ab-a>ab-b$，因而

$$\frac{a(b-1)}{2b}>\frac{ab-b}{2b}=\frac{a-1}{2} \qquad (9.18)$$

注意到$\frac{1}{2}(a-1)$为整数，由(17)、(18)式就得到

$$m=\left[\frac{a(b-1)}{2b}\right]=\frac{a-1}{2} \qquad (9.19)$$

于是再由

$$\left[\frac{n}{b}\right]=\left[\frac{b-1}{2b}\right]=0$$

即从(9.16)式推出恒等式

$$\sum_{j=1}^{\frac{1}{2}(b-1)}[aj/b]+\sum_{k=1}^{\frac{1}{2}(a-1)}[bk/a]$$
$$=\frac{1}{2}(a-1)\cdot\frac{1}{2}(b-1) \qquad (9.20)$$

(9.20)式在证明初等数论中著名的高斯二次互反律时有重要的作用。

我们在行将结束不定方程与恒等式的章节时，特别要谈谈我们的已故导师华罗庚教授在他晚年时的一份未发表的手稿*. 他在这份手稿中，

---

* 华罗庚，关于哥德巴赫问题的一个直接尝试，手稿(1979年10月曾在英国剑桥大学报告过)。(尚未发表)。

建立了一个处理哥德巴赫猜想的直接方法。这是不同于后面要介绍的筛法的一个新尝试。他的思想正是应用了一个关于不定方程解数的初等公式，藉恒等式转化而展开的。基本思路是：

(i)将不定方程

$$ax+by=N,\ a>0,\ b>0,\ (a,b)=1 \tag{9.21}$$

的非负解数记为$R(N;a,b)$，则

$$R(N;a,b)=\frac{N}{ab}+1-\left\{\frac{b^*N}{a}\right\}-\left\{\frac{a^*N}{b}\right\} \tag{9.22}$$

其中$\{x\}$表示x的分数部分。而a^*，b^*为满足下列同余方程的解：

$$aa^*\equiv1(\bmod b),bb^*\equiv1(\bmod a) \tag{9.23}$$

而所谓同余式$A\equiv B(\bmod m)$是指：整数A与B被m除后所得余数相等。

至于这个不定方程解数公式的正确性，这儿就不细述了。

(ii)令$r(N)$为偶数N表示成两个素数之和的表法数，即哥德巴赫问题的解数。记

$$\mu(n)=\begin{cases}1, & 若n=1,\\ (-1)^r, & 若n为r个不同素数之积,\\ 0, & 若n为一素数之平方所整除者。\end{cases}$$

称为莫比乌斯(Möbius)函数。那么就有

$$r(N)=\sum_{A+B=N}\sum_{a\mid(A,H)}\sum_{b\mid(B,H)}\mu(a)\mu(b)$$

$$+\Delta_N) \qquad (9.24)$$

这里(A,H)表A和H的最大公因数，H为不超过$\sqrt{N}$的所有素数的乘积，即

$$H=\prod_{p<\sqrt{N}}p,\quad p\text{素数} \qquad (9.25)$$

而$|\Delta_N|\leqslant k\sqrt{N}$，$k$为某一常数（有时记为$\Delta_N=O(\sqrt{N})$）

(iii)经$r(N)$式子的恒等式转化（用初等变换），可得

$$r(N)=\sum_{d\mid(H,N)}\sum_{a,b}\sum_{\substack{\mid\frac{H}{d}\\ a,b<N/d\\ (a;b)=1}}\mu(a)\mu(b)$$

$$R\left(\frac{N}{d};a,b\right)+O(\sqrt{N})$$

$$=\Phi_1(N)+\Phi_2(N)+O(\sqrt{N})$$

$$(9.26)$$

其中

$$\Phi_1(N)=N\sum_{d\mid(H,N)}\frac{1}{d}\sum_{a,b}\sum_{\substack{\mid\frac{H}{d}\\ a,b<N/d\\ (a,b)=1}}\frac{\mu(a)}{a}\cdot\frac{\mu(b)}{b}$$

$$(9.27)$$

$$\Phi_2(N)=2\sum_{d\mid(H,N)}\sum_{a,b}\sum_{\substack{\mid\frac{H}{d}\\a,b<N/d\\(a,b)=1}}\mu(a)\mu(b)$$

$$\left(\frac{1}{2}-\left\{\frac{b^*N}{ad}\right\}\right)\qquad(9.28)$$

(iv)华罗庚在手稿中证明了：

$$\Phi_1(N)=\frac{N}{\log^2 N}\mathfrak{S}(N)+O\left(\frac{N\log\log N}{(\log N)^{5/2}}\right)$$

(9.29)

其中

$$\mathfrak{S}(N)=\prod_{p\mid N}\frac{p}{p-1}\prod_{p\nmid N}\left(1-\frac{1}{(p-1)^2}\right)$$

(9.30)

是哥德巴赫问题的奇异级数. $\Phi_1(N)$ 可看成为"主项".如果能证明 $\Phi_2(N)$ 为比 $\Phi_1(N)$ "小得多"的"次项"的话，那么就有 $r(N)>0$，从而 $r(N)\geqslant 1$，即哥德巴赫猜想成立. 问题是如何去研究这个$\Phi_2(N)$的大小? 这是一个值得尝试的未解决的问题. 当然，最近有人将$\Phi_2(N)$分成两项：

$$\Phi_2(N)=\Phi_{21}(N)+\Phi_{22}(N)$$

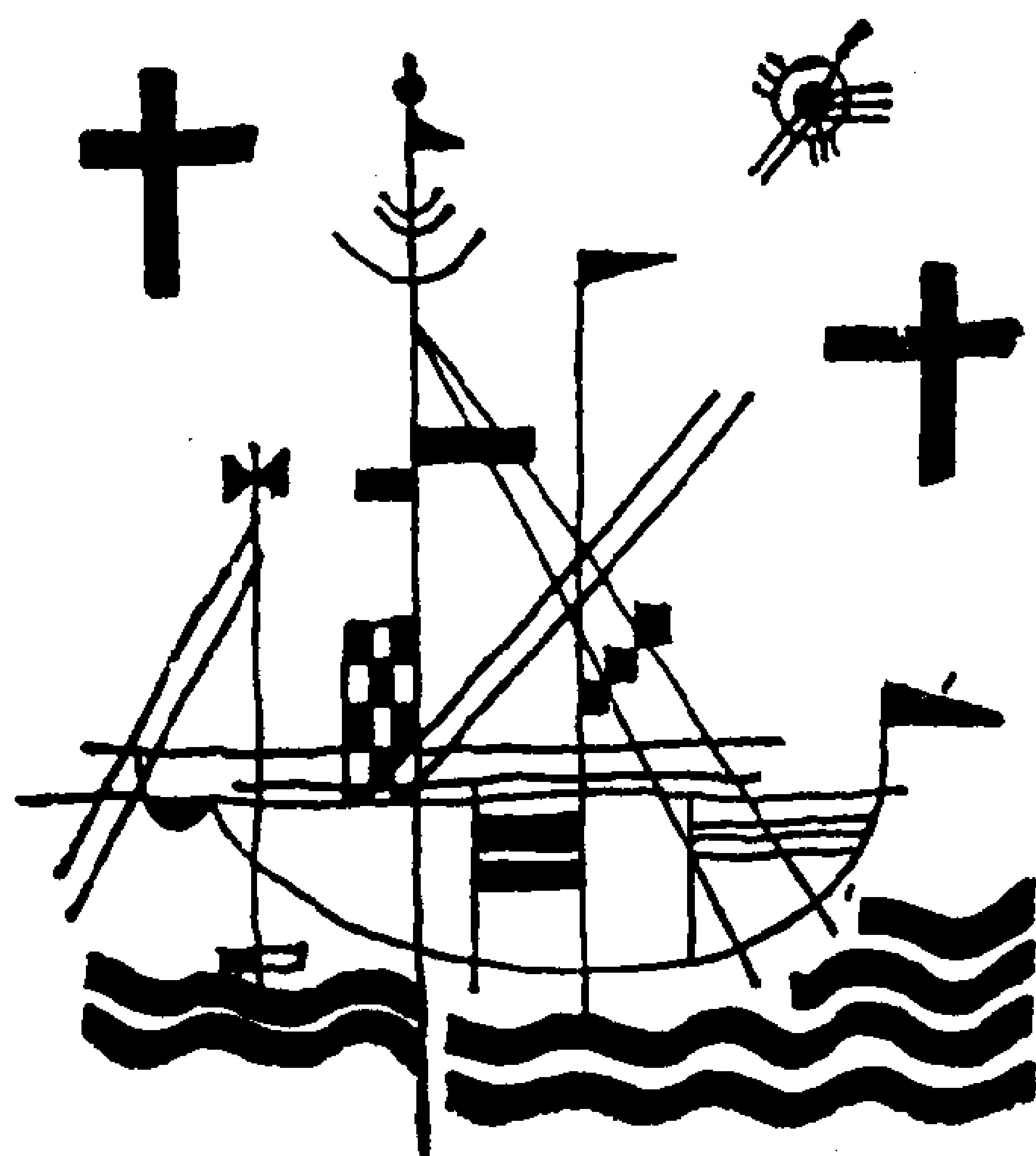
(9.31)

其中一项

$$\Phi_{21}(N)=\sum_{d\mid(H,N)}\sum_{a,b}\sum_{\substack{\mid\frac{H}{d}\\ a,b<N/d\\ (a,b)=1}}\frac{\mu(a)}{a}\mu(b) \tag{9.32}$$

确实证实了是一个“次项”即比$\Phi_1(N)$大约小$\log N$倍之多！但$\Phi_{22}(N)$的情况欠明，仍未得解.（详见：那吉生，关于一个和式的估计，科学通报1986年第9期，641～647页）.

十 哥德巴赫猜想与筛法



我们已经知道，1937年，苏联数学家维诺格拉朵夫利用英国数学家哈代（Hardy)及李特伍德（Littlewood）所创造的圆法以及他自己所独创的三角和方法成功地证明了：每个充分大的奇数皆可表为三个奇素数之和，这就算基本上解决了关于奇数的哥德巴赫猜想。但是这些方法应用于关于偶数的哥德巴赫猜想时却遇到了难以克服的障碍。为此，数学家们一直寻求新的有效方法来研究关于偶数的哥德巴赫猜想。到目前为止，对研究关于偶数的哥德巴赫猜想最为有效且获得最好结果的方法正是筛法。在这一章里我们只能对最最简单的筛法作一介绍，对一这方法有兴趣的读者可以参看哈尔伯斯基与李希特合著的《Sieve Methods（筛法）》一书。这本书是自挪威数学家布朗于1920年左右发明布朗筛法到1973年本书

作者之一正式发表(1＋2)详细证明止这五十多年间筛法理论的系统总结，并附有详尽的参考文献目录，可供有志掌握这一方法的大学高年级学生、研究生等阅读。

为了介绍筛法，首先引进若干记号、术语和必要的数论知识。

符号Σ称为求和号，例如

数计算乘积，例如

$$\sum_{n=1}^{m} f(n)$$

就表示 $f(1)+f(2)+\cdots+f(m)$。而

$$\sum_{\substack{n=1\\(n,r)=1}}^{m} f(n)$$

则表示经过$1,2,\cdots,m$ 当中与 r 互素（若整数 a 与 b 的最大公约数为1，则称 a 与 b 为互素）的自然数求和。例如

$$\sum_{\substack{n=1\\(n,2)=1}}^{10} f(n)=f(1)+f(3)+f(5)+f(7)+f(9)$$

符号Π称为乘积号，例如

$$\prod_{n=1}^{m} f(n)$$

就表示 $f(1)\cdot f(2)\cdot\cdots\cdot f(m)$。而

$$\prod_{\substack{n=1\\(n,r)=1}}^{m} f(n)$$

则表示经过 $1,2,\cdots,m$ 中与 r 互素的那种自然

数计算乘积，例如

$$\prod_{\substack{n=1\\(n,6)=1}}^{15} f(n)=f(1)\cdot f(5)\cdot f(7)\cdot f(11)\cdot f(13).$$

设S是一个集合，我们常记成

$$S=\{a:\cdots\cdots\}$$

这表示S是由所有具备省略号所在位置所述的性质的那种元素a所组成的集合. 例如

$$S_1=\{a:1\leqslant a\leqslant N, 2|a\}$$

就表示由$1,2,\cdots,N$中所有能被2整除的整数a组成之集合S_1，即$1,2,\cdots,N$中全部偶数组成的集合，这里$2|a$表示2整除a.

由有限多个元素组成的集合称为一个有限集，象上面定义的S_1即为一有限集. 对有限集S，我们用$|S|$表示S中元素的个数，例如

$$|S_1|=\left[\frac{N}{2}\right]$$

这里$\left[\frac{N}{2}\right]$表示不超过$\frac{N}{2}$的最大整数. 比如$N=9$时有$|S_1|=[9/2]=4$，$N=10$时$|S_1|=\left[\frac{10}{2}\right]=5$.

我们经常用字母$\mathscr{A}$表示一个有限整数集合：

$$\mathscr{A}=\{a:a\text{ 具有性质}\cdots\cdots\}$$

而用$\mathscr{A}_d$表示$\mathscr{A}$中能被d整除的那种元素组成的集合，即是说

$$\mathscr{A}_d=\{a:a\in\mathscr{A},\ d|a\}$$

这里 $a\in\mathscr{A}$ 表示元素 a 属于 $\mathscr{A}$，也即 a 在集合 $\mathscr{A}$ 中。

下面举几个在筛法中经常遇到的有限整数集合的例子。

例10.1　设 x,y 为实数，$1<y\leqslant x$，定义

$$\mathscr{A}=\{n: x-y<n\leqslant x\}$$

则 $\mathscr{A}$ 就表示在 $x-y$（不含 $x-y$ 本身）与 x（含 x 在内）之间的（正）整数 n 组成之集合。于是

$$|\mathscr{A}|=[x]-[x-y]$$

而对整数 $d\geqslant1$ 有

$$\mathscr{A}_d=\{n: x-y<n\leqslant x, d|n\}$$

因此容易看出（令 $n=dm$）

$$\mathscr{A}_d=\left\{m: \frac{x-y}{d}<m\leqslant\frac{x}{d}\right\}$$

从而

$$|\mathscr{A}_d|=\left[\frac{x}{d}\right]-\left[\frac{x-y}{d}\right] \tag{10.1}$$

假设 $x=dq_1+r_1$，$0\leqslant r_1<d, y=dq_2+r_2$，$0\leqslant r_2<d$，则

$$\left[\frac{x}{d}\right]=q_1 \tag{10.2}$$

$$\left[\frac{x-y}{d}\right]=\left[q_1-q_2+\frac{r_1-r_2}{d}\right] \tag{10.3}$$

如果 $r_1\geqslant r_2$，那么 $0\leqslant r_1-r_2\leqslant r_1<d$，故此时有

$$\left[\frac{x-y}{d}\right]=q_1-q_2 \tag{10.4}$$

如果 $r_1<r_2$，则 $0>r_1-r_2$ 且 $0<r_2-r_1<r_2<d$，

因此

$$\left[\frac{x-y}{d}\right]=q_1-q_2-1 \qquad (10.5)$$

所以有

$$|\mathscr{A}_d|=\begin{cases}q_2=\dfrac{y}{d}-\dfrac{r_2}{d}, & r_1\geqslant r_2 \text{ 时}\\ q_2+1=\dfrac{y}{d}+\dfrac{d-r_2}{d}, & r_1<r_2\text{时}\end{cases}$$

合起就有

$$|\mathscr{A}_d|=\frac{y}{d}+\theta,\ |\theta|\leqslant 1 \qquad (10.6)$$

例10.2 定义

$\mathscr{A}=\{p+2:p\leqslant x\}$，$p$ 表示素数。

于是

$$\mathscr{A}_d=\{p+2:p\leqslant x, d|(p+2)\}$$

如果 d 是偶数，那么 $2|d$，故 $2|(p+2)$，但也有 $2|2$，因此 2 整除 $(p+2)-2=p$，由于 p 是素数，故只可能 $p=2$。于是 d 为偶数时必须 $p=2$，此时 $p+2=4$，它的因数只可能是 1，2，4．因此得到

$$|\mathscr{A}_d|=\begin{cases}1, & d=2 \text{ 或 } 4 \text{ 时}\\ 0, & 2|d \text{ 且 } d\geqslant 6\text{时}\end{cases}$$

当 d 为奇数时，计算 $|\mathscr{A}_d|$ 就不是个简单的事了。由 $d|(p+2)$ 可以假设 $p+2=dm$，于是 $p=dm-2$，于是这时问题就变为求不超过 x 而且具有 $dm-2$ 形状的素数个数。这种形状的素数都在首项为 -2、公差为 d 的算术级数之中。由于

$2\nmid d$，一个著名的狄里希莱定理告诉我们：在这种算术级数中必有无穷多个素数（事实上更一般地可以证明，当整数 k 与 l 互素时，在以 l 为首项、k 为公差的算术级数中必有无穷多个素数存在）．而且在不超过 x 这一段中大约有

$$\frac{x}{\varphi(d)\ln x}$$

个这种素数（在上述一般情形，在不超过 x 这一段中有近似

$$\frac{x}{\varphi(k)\ln x}$$

个这种素数）。其中 $\varphi(d)$称为 d 的尤拉 φ 函数．它定义如下。

定义10.1 对任何正整数 n，$\varphi(n)$表示 $1,\cdots,n$ 这 n 个数中与 n 互素的整数的个数．

例如：$\varphi(1)=1$，$\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$。

由于 1，2，…，2^k 中任一个奇数皆与 2 互素，当然也与 2^k 互素，又因为 $1,2,\cdots,2^k$中的奇数个数恰好占一半，即 $2^k/2=2^{k-1}$ 个，因此对任何整数 $k\geqslant1$ 有

$$\varphi(2^k)=2^{k-1}$$

对任何素数p，显然$1,\cdots,p-1$这 $p-1$个数皆与p互素，因为p的正因数只能是 1 和p。所以就有

$$\varphi(p)=p-1$$

任一个整数m若与素数p互素，当然也必与p^s（$s\geqslant 1$为整数）互素，反过来也对。而m与p是不是互素，只要看p能不能整除m即可，详细说来就有：m与p^s互素，当且仅当$p\nmid m$。由于$1,2,\cdots,p^s$这p^s个数中恰有$p^s/p=p^{s-1}$个数能被p整除，除去这p^{s-1}个数剩下的数就一定与p^s互素了，因此得到

$$\varphi(p^s)=p^s-p^{s-1} \tag{10.7}$$

为了进一步研究象尤拉φ函数这种函数的性质，我们需要一些概念。

定义10.2 定义域为正整数集合（简记为Z^+）而取值为复数（简记复数集合为C）的函数称为一个算术函数（或称为数论函数）。

定义10.3 设$f(n)$为一个算术函数，如果对任何一对正整数$m,n,(m,n)=1$，皆有$f(mn)=f(m)f(n)$，则称$f(n)$是一个积性函数。如果对任一对正整数m,n，不论它们是否互素，都有$f(mn)=f(m)f(n)$，那么就称$f(n)$是一个完全积性函数。

例如，$f(n)=n$是一个完全积性函数，$f(n)=\ln n$就不是积性函数，因为

$$\ln(1\cdot 2)=\ln 2\neq 0$$

而
$$(\ln 1)(\ln 2)=0$$

故　　$\ln(1\cdot 2)\neq(\ln 1)(\ln 2)$

若 $f(n)$ 是积性的，且其值不恒为 0，那么一定有 $f(1)=1$。这是因为由假设，存在至少一个正整数 n_0 使 $f(n_0)\neq 0$，由积性有

$$f(n_0)=f(1\cdot n_0)=f(1)f(n_0)$$

但因为 $f(n_0)\neq 0$，故得 $f(1)=1$

可以证明，函数 φ 就是一个积性函数。设 $f(n)$ 为一个积性函数，对每个整数 $n>1$，设它的标准分解式为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}.$$

这里一切 α_i，$1\leqslant i\leqslant s$ 为正整数，诸 $p_i\ (1\leqslant i\leqslant s)$ 为互不相同的素数。则由 $p_1^{\alpha_1}$ 与 $p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 互素，我们有

$$f(n)=f(p_1^{\alpha_1})f(p_2^{\alpha_2}\cdots p_s^{\alpha_s})$$

继续使用这一方法可得

$$f(n)=f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_s^{\alpha_s})=\prod_{i=1}^{s}f(p_i^{\alpha_i})\qquad(10.8)$$

特别取 φ 函数即得到

$$\varphi(n)=\prod_{i=1}^{s}\varphi(p_i^{\alpha_i})=\prod_{i=1}^{s}(p_i^{\alpha_i}-p_i^{\alpha_i-1})=\prod_{i=1}^{s}p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)$$

$$= n\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right) \qquad (10.9)$$

这里用到（10.7）式。

下面再介绍一个重要的算术函数。

定义10.4* 定义莫比乌斯 μ 函数如下：

$$\mu(n)=\begin{cases}1, & \text{当 } n=1 \text{ 时}\\ 0, & \text{当 } n \text{ 有平方因数时}\\ (-1)^s, & \text{当 } n=p_1p_2\cdots p_s \text{ 时}\end{cases}$$

其中 $p_1,\cdots,p_s$ 为互不相同之素数。

我们来证 $\mu(n)$ 是积性函数。设 n 与 m 是两个互素的正整数。

如果 $n=1$，显然有

$$f(nm)=f(m)=f(1)f(m)=f(n)f(m)$$

当 $m=1$ 时也同样可证。故可以设 $n>1,m>1$ 而且 $(n,m)=1$。

如果 n 与 m 中至少有一个数有平方因数，不妨可以设 n 有平方因数，那么由定义有 $\mu(n)=0$。又容易看出 nm 也有平方因数，于是也有 $\mu(nm)=0$，从而有

$$\mu(nm)=0=0\cdot\mu(m)=\mu(n)\mu(m)$$

最后讨论 n 与 m 都没有平方因数的情形。可设 $n=p_1\cdots p_s, m=q_1\cdots q_t$，这里 $p_1,\cdots p_s$ 为 s（$s\geqslant$

---

* 这个函数的定义，我们曾在第九章末介绍过。

1）个不同的素数，$q_1,\cdots,q_t$ 为 $t(t\geqslant 1)$ 个不同的素数。由 $(n, m)=1$ 立即看出，$p_1, \cdots, p_s$ 与 $q_1, \cdots, q_t$ 合在一起是 $s+t$ 个互不相同的素数集合。因而由定义10.4就有

$$\mu(nm)=(-1)^{s+t}=(-1)^s\cdot(-1)^t$$
$$=\mu(n)\mu(m)$$

这就证明了$\mu(n)$是积性算术函数。

莫比乌斯函数有如下重要的性质。

$$\sum_{d\mid n}\mu(d)=\begin{cases}1, & n=1\text{ 时}\\ 0, & n>1\text{ 时}\end{cases} \quad (10.10)$$

这里求和记号 $d\mid n$ 表示经过 n 的所有正因数 d 求和。例如$n=15$时，其全部正因数为如下4个：

1，3，5，15

于是

$$\sum_{d\mid 15}\mu(d)=\mu(1)+\mu(3)+\mu(5)+\mu(15)$$
$$=1+(-1)+(-1)+(-1)^2$$
$$=0$$

下面来证明（10.10）式。

$n=1$ 时 n 只有 $d=n=1$ 这一个正因数，而 $\mu(1)=1$，故此时结论成立。

$n>1$ 时可设其标准分解式为 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，则 n 的全部正因数如下所示：

1）$d=1$，　　相应有 $\mu(1)=1$。

2）$d=p_1,\cdots,p_s$，相应有 $\mu(p_1)=\cdots=\mu(p_s)=-1$，个数有 s 个，合之得 $s\cdot(-1)$。

3）$d=p_1p_2,\cdots,p_1p_s$，

$$\cdots\cdots\cdots\cdots$$

$$p_{s-1}p_s,$$

相应每项 p_ip_j 得到 $\mu(p_ip_j)=(-1)^2=1$，总共这样的因数有 $\binom{s}{2}$ 个，故得 $\binom{s}{2}$。

…………

最后，$d=p_1\cdots p_s$ 也是 n 的正因数，总共只有 $\binom{s}{s}=1$ 个这种正因数。对应这个因数的函数值为 $\mu(p_1\cdots p_s)=(-1)^s$。

4）剩下的正因数如果还有的话，一定是有平方因数的了，对这种正因数 d 有 $\mu(d)=0$。

合起来得到

$$\sum_{d\mid n}\mu(d)=1+\binom{s}{1}(-1)+\binom{s}{2}(-1)^2+\cdots+\binom{s}{s}(-1)^s=(1-1)^s=0.$$

这里用到二项展开公式($s\geqslant1$)

$$(a-b)^s=a^s+\binom{s}{1}(-b)a^{s-1}+\binom{s}{2}(-b)^2a^{s-2}+\cdots+\binom{s}{s}(-b)^s$$

下面来定义筛集$\mathscr{T}$和筛函数 S。

所谓筛集$\mathscr{T}$，是由无穷多个素数组成的一个

集合（其中没有相同的元素出现），用$\overline{\mathscr{T}}$表示全体不属于$\mathscr{T}$的素数组成的集合。用$\mathscr{T}(k)$表示$\mathscr{T}$中所有不能整除k的素数组成的集合，即

$$\mathscr{T}(k)=\{p:p\in\mathscr{T},p\nmid k\}.$$

设$z\geqslant2$为一个实数。定义

$$P(z)=\prod_{\substack{p<z\\p\in\mathscr{T}}}p$$

即$P(z)$表示$\mathscr{T}$中小于z的全部素数的乘积。

筛函数S由下式定义

$$S(\mathscr{A};\mathscr{T},z)=\sum_{\substack{a\in A\\(a,P(z))=1}}1$$

即是说$S(\mathscr{A};\mathscr{T},z)$表示集合$\mathscr{A}$中与$P(z)$互素的整数的个数。换言之，就是用$\mathscr{T}$中小于$z$的素数组成的集合

$$\mathscr{T}(z)=\{p:p\in\mathscr{T},p<z\}$$

作成一个"筛子"，将$\mathscr{A}$中的数都过这张"筛子"筛一筛，凡与$\mathscr{T}(z)$中元素有大于1的公因数的那种数$a\in\mathscr{A}$即被筛掉，而经筛选后留下的数都是与$\mathscr{T}(z)$中的素数互素的数。

下面来举一例说明我们的想法。

取集合

$$\mathscr{A}=\{n:n\leqslant x\}$$

取$\mathscr{T}$为所有素数组成之集合。于是$S(\mathscr{A};\mathscr{T},z)$就表示不超过$x$的正整数中不能被小于$z$的素数

整除的那种正整数的个数。

由定义及莫比乌斯函数的性质（见（10.10）式）就有

$$
\begin{aligned}
S(\mathscr{A};\mathscr{T},z) &= \sum_{\substack{a\in\mathscr{A}\\(a,P(z))=1}} 1\\
&= \sum_{a\in\mathscr{A}}\ \sum_{d\mid(a,P(z))} \mu(d)\\
&= \sum_{a\in\mathscr{A}}\ \sum_{\substack{d\mid a\\ d\mid P(z)}} \mu(d) \qquad (10.11)
\end{aligned}
$$

交换求和次序得到

$$
\begin{aligned}
S(\mathscr{A};\mathscr{T},z) &= \sum_{d\mid P(z)} \mu(d) \sum_{\substack{a\in\mathscr{A}\\ d\mid a}} 1\\
&= \sum_{d\mid P(z)} \mu(d)\,|\mathscr{A}_d| \qquad (10.12)
\end{aligned}
$$

由本章开始的例10.1（在那里令 $x=y$，然后再将字母 y 改写成 x）立即得到

$$
S(\mathscr{A};\mathscr{T},z) = x\sum_{d\mid P(z)} \frac{\mu(d)}{d} + \sum_{d\mid P(z)} \mu(d)\theta \qquad (10.13)
$$

式中 $|\theta|\leqslant 1$.

记（10.13）式右边第二个和为R，由于恒有$|\mu(d)|\leqslant 1$ 以及 $|\theta|\leqslant 1$，故有

$$
|R| \leqslant \sum_{d\mid P(z)} 1 \qquad (10.14)
$$

由于$P(z)$是小于z的所有素数之积，而这种素数个数显然小于$[z]$个。与证明（10.10）式同样

地可以证出，$P(z)$的所有正因数d的个数恰为$(1+1)^m$个，这里m为小于z的素数个数，于是

$$|R|\leqslant(1+1)^m=2^m\leqslant 2^{[z]}\leqslant 2^z \tag{10.15}$$

利用乘法及函数μ之定义不难证明

$$\sum_{d\mid P(z)}\frac{\mu(d)}{d}=\prod_{p\mid P(z)}\left(1-\frac{1}{p}\right)=\prod_{p<z}\left(1-\frac{1}{p}\right) \tag{10.16}$$

为了进一步讨论，需要下面两个引理。

引理10.1 对任何$1>x>0$有$\ln(1-x)<-x$。

学过微积分的读者可以应用函数的导数与函数单调性的联系来证明这个结论，这里我们略去详细证明。

引理10.2 存在常数$B_1>0$，$B_2>0$使当z充分大时有

$$\sum_{p<z}\frac{1}{p}>\ln\ln z+B_1 \tag{10.17}$$

$$\sum_{p<z}\frac{1}{p}<\ln\ln z+B_2 \tag{10.18}$$

由引理10.1及引理10.2容易有，当z充分大时

$$\ln\prod_{p<z}\left(1-\frac{1}{p}\right)=\sum_{p<z}\ln\left(1-\frac{1}{p}\right)<-\sum_{p<z}\frac{1}{p}<-\ln\ln z-B_1$$

由此立即推出

$$\prod_{p<z}\left(1-\frac{1}{p}\right)<e^{-\ln\ln z}=\frac{1}{\ln z} \quad (10.19)$$

注意到$\mathscr{A}$中小于z的素数也都被筛掉了，这种素数个数不超过z，于是由（10.13），（10.14），（10.15），（10.16）以及（10.19）式就得到，当z充分大时

$$\pi(x)\leqslant z+S(\mathscr{A};\mathscr{T},z)<\frac{x}{\ln z}+2^z+z \quad (10.20)$$

特别取$z=\ln x$就得到

$$\pi(x)<\frac{x}{\ln\ln x}+2^{\ln x}+\ln x$$

$$=\frac{x}{\ln\ln x}\left(1+\frac{2^{\ln x}\ln\ln x}{x}+\frac{(\ln x)(\ln\ln x)}{x}\right) \quad (10.21)$$

当x充分大时我们有

$$\frac{2^{\ln x}\ln\ln x}{x}=\frac{x^{\ln 2}\ln\ln x}{x}<\frac{\ln\ln x}{x^{0.3}}<\frac{1}{2}$$

$$\frac{(\ln x)(\ln\ln x)}{x}<\frac{\ln\ln x}{\sqrt{x}}<\frac{1}{2}$$

合起来就有，当x充分大时有

$$\pi(x)<\frac{2x}{\ln\ln x} \quad (10.22)$$

由此可以给出一个简单的推论：当 $x\to+\infty$ 时 $\pi(x)/x\longrightarrow 0$。

上面所用的筛法称为爱拉托士散纳——勒让德筛法。但是这个方法过于粗糙，因而给出的结果常常比较差。拿上面 $\pi(x)$的估计式(10.22)来说，只需要用到二项式系数$\binom{m}{n}$的简单性质，就可以证出有形如

$$\alpha\frac{x}{\ln x}<\pi(x)<\beta\frac{x}{\ln x} \qquad (10.23)$$

的不等式成立，这里 $\alpha>0$，$\beta>0$ 为常数。显然(10.23) 比 (10.22) 要更加接近真实的结果

$$\pi(x)\sim\frac{x}{\ln x} \qquad (10.24)$$

(这里 $f(x)\sim g(x)$表示$f(x)/g(x)\to 1$ ($x\to+\infty$ 时))

但是，经过布朗和塞尔伯格等人的改造，筛法却超越许多其它方法，成为数论近代研究中一个重要的工具。下面我们要来简单介绍一下塞尔伯格上界筛法。为此要先给出若干定义及准备知识。

定义 X 为集合$\mathscr{A}$中元素个数$|\mathscr{A}|$的一个比较好而且便于应用的近似值。例如在例10.1中可以取 $X=y$

在一般情形，X可以有多种不同的取法，一般说来，选取X需要遵循两条原则：

1）X的表达式要简单，便于应用。

2）误差$r_1=|\mathscr{A}|-X$的绝对值要小，便于误差项估计时可以得到较好的结果。

对于$|\mathscr{A}_d|$，这里$(d,\overline{\mathscr{T}})=1$ 且$\mu(d)\neq 0$（即d没有平方因数，而且d没有$\mathscr{T}$以外的素因数）．在很多情形中，常常可以找到一个非负积性函数$\omega(d)$，使得$\dfrac{\omega(d)}{d}X$可以作为$|\mathscr{A}_d|$的一个合适的近似值。记误差为

$$r_d=|\mathscr{A}_d|-\frac{\omega(d)}{d}X \qquad (10.25)$$

例如在所给的例10.1中，可取$X=y$，再由(10.6)式知可以取$\omega(d)=1$。相应有$r_d=\theta$，$|\theta|\leqslant 1$。

由$\omega(d)$可以定义以下几个函数：

$$W(z)=\prod_{p<z}\left(1-\frac{\omega(p)}{p}\right) \qquad (10.26)$$

$$g(d)=\frac{\omega(d)}{d\prod\limits_{p\mid d}\left(1-\dfrac{\omega(p)}{p}\right)},\quad \mu(d)\neq 0$$

$$(10.27)$$

$$G(z)=\sum_{\substack{d<z\\ d\mid P(z)}}\mu^2(d)g(d) \qquad (10.28)$$

$$G_k(z)=\sum_{\substack{d<z\\ (d,k)=1\\ d\mid P(z)}}\mu^2(d)g(d) \qquad (10.29)$$

为了简单起见，我们总假定$\omega(d)$满足条件

$$0<\frac{\omega(p)}{p}\leqslant 1-\frac{1}{L_1},\ (p,\ \overline{\mathscr{T}})=1 \tag{10.30}$$

其中 L_1 为一个大于 1 的常数，在很多情形，可以取到 $\omega(d)$ 使（10.30）得到满足。

设 $\lambda_1=1$，对 $d\geqslant z$ 有 $\lambda_d=0$。则有（对每个 $a\in\mathscr{A}$）

$$\sum_{\substack{d\mid a\\ d\mid P(z)}}\mu(d)\leqslant\Big(\sum_{\substack{d\mid a\\ d\mid P(z)}}\lambda_d\Big)^2 \tag{10.31}$$

这是因为

$$\sum_{\substack{d\mid a\\ d\mid P(z)}}\mu(d)=\begin{cases}1 &, \text{当}(a,P(z))=1\text{时}\\ 0 &, \text{当}(a,P(z))>1\text{时}\end{cases}$$

而由 $\lambda_1=1$ 有

$$\Big(\sum_{\substack{d\mid a\\ d\mid P(z)}}\lambda_d\Big)^2=\begin{cases}\lambda_1=1, \text{当}(a,P(z))=1\text{时}\\ C\geqslant 0, \text{当}(a,p(z))>1\text{时}\end{cases}$$

于是就有

$$\begin{aligned}S(\mathscr{A};\mathscr{T},z)&=\sum_{\substack{a\in\mathscr{A}\\ (a,P(z))=1}}1=\sum_{a\in\mathscr{A}}\ \sum_{\substack{d\mid a\\ d\mid P(z)}}\mu(d)\\ &\leqslant\sum_{a\in\mathscr{A}}\Big(\sum_{\substack{d\mid a\\ d\mid P(z)}}\lambda_d\Big)^2\\ &=\sum_{a\in\mathscr{A}}\Big(\sum_{\substack{d_1\mid a\\ d_1\mid P(z)}}\lambda_{d_1}\Big)\Big(\sum_{\substack{d_2\mid a\\ d_2\mid P(z)}}\lambda_{d_2}\Big)\\ &=\sum_{\substack{d_1\mid P(z)\\ d_2\mid P(z)}}\lambda_{d_1}\lambda_{d_2}\sum_{\substack{a\in\mathscr{A}\\ d_1\mid a\\ d_2\mid a}}1\end{aligned} \tag{10.32}$$

用 $[d_1,d_2]$ 表示 d_1 与 d_2 之最小公倍数，易见

$$d_1|a,\ d_2|a$$

就等价于

$$[d_1,d_2]|a$$

而由（10.25）式有

$$\sum_{\substack{a\in\mathscr{A}\\ [d_1,d_2]|a}} 1 = |\mathscr{A}_{[d_1;d_2]}|$$

$$= \frac{\omega([d_1,d_2])}{[d_1,d_2]}X + r_{[d_1;d_2]} \tag{10.33}$$

引理10.3 设m,n为任二正整数，则

$$[m,n](m,n)=mn$$

证明 设$(m,n)=r$，$m=rm_1$，$n=rn_1$，则$(m_1,n_1)=1$，而且容易看出，rm_1n_1正是m与n之最小公倍数，即$[m,n]=rm_1n_1$。于是

$$[m,n](m,n)=(rm_1n_1)(r)=(rm_1)(rn_1)$$
$$=mn$$

引理10.4 设f为一个积性算术函数，则对任何正整数m，n，$\mu(m)\neq 0,\mu(n)\neq 0$，皆有

$$f([m,n])f((m,n))=f(m)f(n)$$

证明 仍设$(m,n)=r,m=rm_1,n=rn_1$，则$(m_1,n_1)=1$。由于$\mu(m)\neq 0,\mu(n)\neq 0$，故$m$与$n$皆无平方因数，从而必有$(r,m_1)=1,(r,n_1)=1$。于是也有

$$(rm_1,n_1)=1,\ (rn_1,m_1)=1$$

由 f 的积性立即得到

$$f([m,n])=f(rm_1\cdot n_1)=f(rm_1)f(n_1)$$

再由$(r,n_1)=1$ 即得

$$f((m,n))f(n_1)=f(r)f(n_1)=f(rn_1)$$

合起来就得到

$$f([m,n])f((m,n))=f(rm_1)f(rn_1)$$
$$=f(m)f(n)$$

特别地取 $f(d)=\omega(d)$就得到

$$\frac{\omega([d_1,d_2])}{[d_1,d_2]}=\frac{\omega(d_1)\omega(d_2)}{\omega((d_1,d_2))}\cdot\frac{1}{[d_1,d_2]} \tag{10.34}$$

由引理10.3有

$$[d_1,d_2]=\frac{d_1d_2}{(d_1,d_2)} \tag{10.35}$$

由（10.34）、（10.35）式得到

$$\frac{\omega([d_1,d_2])}{[d_1,d_2]}=\frac{\omega(d_1)\omega(d_2)}{d_1d_2}\cdot\frac{(d_1,d_2)}{\omega((d_1,d_2))} \tag{10.36}$$

由（10.32）、（10.33）以及（10.36)式得到

$$S(\mathscr{A};\mathscr{T},z)\leqslant XT+R \tag{10.37}$$

这里

$$T=\sum_{\substack{d_1|P(z)\\d_2|P(z)}}\lambda_{d_1}\lambda_{d_2}\frac{\omega(d_1)\omega(d_2)(d_1,d_2)}{d_1d_2\omega((d_1,d_2))}. \tag{10.38}$$

$$R=\sum_{\substack{d_1\mid P(z)\\ d_2\mid P(z)}}|\lambda_{d_1}\lambda_{d_2}r_{[d_1,d_2]}| \qquad (10.39)$$

由（10.27）式有

$$g(p)=\frac{\omega(p)}{p\left(1-\frac{\omega(p)}{p}\right)}=\frac{\omega(p)}{p-\omega(p)}$$

于是

$$\frac{1}{g(p)}=\frac{p-\omega(p)}{\omega(p)}=\frac{p}{\omega(p)}-1$$

故有

$$\frac{p}{\omega(p)}=1+\frac{1}{g(p)} \qquad (10.40)$$

对任给正整数 d，$\mu(d)\neq 0$，利用乘法及(10.40)式容易证明有

$$\frac{d}{\omega(d)}=\prod_{p\mid d}\frac{p}{\omega(p)}=\prod_{p\mid b}\left(1+\frac{1}{g(p)}\right)$$

$$=\sum_{l\mid d}\frac{1}{g(l)}. \qquad (10.41)$$

特别取 $d=(d_1, d_2)$得到

$$\frac{(d_1, d_2)}{\omega((d_1, d_2))}=\sum_{l\mid(d_1,d_2)}\frac{1}{g(l)}=\sum_{\substack{l\mid d_1\\ l\mid d_2}}\frac{1}{g(l)} \qquad (10.42)$$

由（10.38）、（10.42）式得到

$$T=\sum_{\substack{d_1\mid P(z)\\ d_2\mid P(z)}}\lambda_{d_1}\lambda_{d_2}\frac{\omega(d_1)\omega(d_2)}{d_1d_2}\sum_{\substack{l\mid d_1\\ l\mid d_2}}\frac{1}{g(l)}$$

$$=\sum_{l\mid P(z)}\frac{1}{g(l)}\left(\sum_{\substack{d_1\mid P(z)\\ l\mid d_1}}\lambda_{d_1}\frac{\omega(d_1)}{d_1}\right)$$

$$\left(\sum_{\substack{d_2 \mid P(z) \\ l \mid d_2}} \lambda_{d_2} \frac{\omega(d_2)}{d_2}\right)$$

$$= \sum_{l \mid P(z)} \frac{1}{g(l)} y_l^2 \qquad (10.43)$$

这里定义

$$y_l = \sum_{\substack{d \mid P(z) \\ l \mid d, d<z}} \lambda_d \frac{\omega(d)}{d} \qquad (10.44)$$

下面要选取适当的 λ_d，使得 T 取到最小值。定义

$$F = \sum_{d<z, d \mid P(z)} \mu(d) y_d \qquad (10.45)$$

由定义（10.44)及莫比乌斯函数的性质(10.10)容易得到

$$F = \sum_{\substack{d<z \\ d \mid P(z)}} \mu(d) \sum_{\substack{r \mid p(z) \\ d \mid r}} \lambda_r \frac{\omega(r)}{r}$$

$$= \sum_{r \mid P(z)} \lambda_r \frac{\omega(r)}{r} \sum_{\substack{d<z \\ d \mid r}} \mu(d)$$

$$= \sum_{r \mid P(z)} \lambda_r \frac{\omega(r)}{r} \sum_{d \mid r} \mu(d)$$ （因为 $r \geqslant z$ 时 $\lambda_r = 0$)

$$= \lambda_1 \frac{\omega(1)}{1} = 1 \qquad (10.46)$$

最后一步用到 $\lambda_1 = 1$ 以及 ω 是不恒为 0 的积性函数，故必有 $\omega(1) = 1$。

可以证明（见附录），在限制条件(10.46)

之下，使T取极值的λ_d由下式定义：

$$\lambda_d=\frac{\mu(d)}{\prod\limits_{p\mid d}\left(1-\frac{\omega(p)}{p}\right)}\cdot\frac{G_d(z/d)}{G(z)}$$

$$d\mid P(z) \qquad (10.47)$$

我们先来验证由（10.47）定义的λ_d满足

$$\lambda_1=1$$

及 $$\lambda_d=0 \quad (d\geqslant z)$$

这两个条件。

首先有

$$\lambda_1=\mu(1)\cdot\frac{G_1(z)}{G(z)}=\mu(1)=1$$

又当 $d\geqslant z$ 时，$z/d\leqslant 1$，故由（10.29）式有$G_d(z/d)=0$，即

$$\lambda_d=0,\quad d\geqslant z \text{ 时}$$

再来证明（10.47）式给出的λ_d确使T取最小值。为此需要应用下面的引理.

引理10.5 设a_n，b_n为实数，$1\leqslant n\leqslant m$，则

$$\left(\sum_{n\leqslant m}a_nb_n\right)^2\leqslant\left(\sum_{n\leqslant m}a_n^2\right)\left(\sum_{n\leqslant m}b_n^2\right).$$

证明 考虑二次三项式

$$\left(\sum_{n\leqslant m}a_n^2\right)x^2+2\left(\sum_{n\leqslant m}a_nb_n\right)x+\left(\sum_{n\leqslant m}b_n^2\right)$$

$$= \sum_{n \leqslant m}\left(a_n^2 x^2 + 2a_n b_n x + b_n^2\right)$$

$$= \sum_{n \leqslant m}(a_n x + b_n)^2 \geqslant 0$$

由于它对任何 x 皆取非负值，且 $\sum\limits_{n \leqslant m} a_n^2 \geqslant 0$，故其判别式必不大于0，即

$$4\left(\sum_{n \leqslant m} a_n b_n\right)^2 - 4\left(\sum_{n \leqslant m} a_n^2\right)\left(\sum_{n \leqslant m} b_n^2\right) \leqslant 0$$

此即所欲证者。

由 $F=1$ 以及引理10.5我们就得到

$$1 = F = \sum_{\substack{d < z \\ d \mid P(z)}} \mu(d) y_d = \left(\sum_{\substack{d < z \\ d \mid P(z)}} \mu(d) y_d\right)^2$$

$$= \left(\sum_{\substack{d < z \\ d \mid P(z)}} \mu(d) \sqrt{g(d)} \frac{y_d}{\sqrt{g(d)}}\right)^2$$

$$\leqslant \left(\sum_{\substack{d < z \\ d \mid P(z)}} \mu^2(d) g(d)\right)\left(\sum_{\substack{d < z \\ d \mid P(z)}} \frac{y_d^2}{g(d)}\right) \qquad (10.48)$$

由定义（10.44）易见，实际上有

$$\sum_{\substack{d < z \\ d \mid P(z)}} y_d^2/g(d)$$

$$= \sum_{d \mid P(z)} y_d^2/g(d) = T \qquad (10.49)$$

于是由（10.48）、（10.49）及（10.28）式就有

$$1 \leqslant G(z) T$$

故得

$$T \geqslant 1/G(z) \qquad (10.50)$$

这证明了，在限制条件 $F=1$ 之下，不论 λ_d 如何选取，皆有（10.50）成立，下面我们要来证明，按照（10.47）式选取的 λ_d 恰使（10.50）式取等号，从而取到最小值 $1/G(z)$。

由定义我们得到

$$y_l=\sum_{\substack{d\mid P(z)\\ l\mid d}}\frac{\omega(d)}{d}\frac{\mu(d)}{\prod\limits_{p\mid d}\left(1-\frac{\omega(p)}{p}\right)}\frac{G_d(z/d)}{G(z)}$$

（10.51）

由（10.40）式有

$$\prod_{p\mid d}\left(1-\frac{\omega(p)}{p}\right)=\prod_{p\mid d}\left(1-\frac{1}{1+\frac{1}{g(p)}}\right)$$

$$=\prod_{p\mid d}\frac{1}{1+g(p)}$$

由（10.41）式有

$$\frac{\omega(d)}{d}=\prod_{p\mid d}\left(1+\frac{1}{g(p)}\right)^{-1}$$

$$=\prod_{p\mid d}\left(\frac{1+g(p)}{g(p)}\right)^{-1}$$

由上二式得

$$\frac{\omega(d)}{d}\cdot\frac{1}{\prod\limits_{p\mid d}\left(1-\frac{\omega(p)}{p}\right)}=\prod_{p\mid d}g(p)=g(d)$$

（10.52）

这里最后一步用到 g 是积性函数，而 $d\mid P(z)$，从

而 d 无平方因数。于是由（10.51）、（10.52）式以及（10.29）式得到

$$y_l=\sum_{\substack{d|P(z)\\ l|d}}\mu(d)g(d)\frac{G_d(z/d)}{G(z)}$$

$$=\frac{1}{G(z)}\sum_{\substack{m|P(z)\\ (m,l)=1}}\mu(lm)g(lm)G_{lm}(Z/lm)$$

$$(\text{令}d=lm)$$

$$=\frac{\mu(l)g(l)}{G(z)}\sum_{\substack{m|P(z)\\ (m,l)=1}}(m)g(m)\sum_{\substack{d<z/lm\\ (d,lm)=1,\,d|P(z)}}\mu^2(d)g(d)$$

$$=\frac{\mu(l)g(l)}{G(z)}\sum_{\substack{m|P(z)\\ (m,l)=1}}\mu(m)\sum_{\substack{d<z/lm\\ (d,lm)=1\\ d|P(z)}}\mu^2(d)\mu^2(m)g(d)g(m)$$

$$=\frac{\mu(l)g(l)}{G(z)}\sum_{\substack{dm<z/l\\ (dm,l)=1\\ d|P(z)}}\mu^2(dm)g(dm)\sum_{m|P(z)}\mu(m)$$

$$=\frac{\mu(l)g(l)}{G(z)}\sum_{\substack{n<z/l\\ (n,l)=1\\ n|P(z)}}\mu^2(n)g(n)\sum_{m|n}\mu(m)$$

$$(\text{令}(n=dm)\qquad\qquad(10.53)$$

这里用到μ与 g 为积性函数的性质，再由(10.10)式就得到

$$y_l=\frac{\mu(l)g(l)}{G(z)}\cdot\mu^2(1)g(1)\mu(1)$$

$$=\frac{\mu(l)g(l)}{G(z)}\qquad\qquad(10.54)$$

由（10.43）及（10.54）式就推出，对所取之λ_d值有

$$T=\sum_{l\mid P(z)}\frac{1}{g(l)}\cdot\left(\frac{\mu(l)g(l)}{G(z)}\right)^2$$

$$=\frac{1}{G(z)^2}\sum_{l\mid P(z)}\mu^2(l)g(l)$$

$$=\frac{G(z)}{G(z)^2}=\frac{1}{G(z)} \qquad (10.55)$$

这正是所要证明的。

为了研究（10.37）式中的余项R，首先来证

引理10.6 设λd由（10.47）式给出，则恒有

$$|\lambda_d|\leqslant 1$$

证明 由定义有

$$G(z)=\sum_{\substack{m\mid P(z)\\ m<z}}\mu^2(m)g(m)$$

$$=\sum_{l\mid d}\sum_{\substack{m<z\\ (m,d)=l\\ m\mid P(z)}}\mu^2(m)g(m)$$

$$=\sum_{\substack{l\mid d\\ l\mid P(z)}}\sum_{\substack{h<z/l\\ (h,d/l)=1\\ (h,l)=1\\ h\mid P(z)}}\mu^2(lh)g(lh)$$

（令 $m=lh$）

$$=\sum_{\substack{l\mid d\\ l\mid P(z)}}\mu^2(l)g(l)\sum_{\substack{h<z/l\\ (h,d)=1\\ h\mid P(z)}}\mu^2(h)g(h)$$

$$\geqslant \sum_{\substack{l \mid d \\ l \mid P(z)}} \mu^2(l) g(l) \sum_{\substack{h < z/d \\ (h,d)=1 \\ h \mid P(z)}} \mu^2(h) g(h)$$

(因为 $l \leqslant d$)

$$= G_d(z/d) \sum_{\substack{l \mid d \\ l \mid P(z)}} \mu^2(l) g(l). \tag{10.56}$$

注意到我们总是对满足 $d|P(z)$的 d 定义 λ_d 的。故最后一式中 $l|P(z)$ 这一条件可以略去。为了进一步化简（10.56）式，我们需要两个引理。

引理10.7 设 f 为不恒为 0 之积性函数，则

$$\sum_{l \mid d} \mu(l) f(l) = \prod_{p \mid d} (1 - f(p))$$

引理10.8 两个积性函数之积仍为积性函数。

这两个引理的证明略去。

由于 μ 与 g 皆为积性函数，由引理10.8知 $\mu(l)g(l)$ 仍为积性函数，对 $f(l) = \mu(l)g(l)$ 应用引理10.7即得

$$\sum_{\substack{l \mid d \\ l \mid P(z)}} \mu^2(l) g(l) = \sum_{l \mid d} \mu(l)(\mu(l) g(l))$$

$$= \prod_{p \mid d} (1 - \mu(p) g(p))$$

$$= \prod_{p \mid d} (1 + g(p)) \quad (因\mu(p) = -1)$$

$$=1/\prod_{p\mid d}\left(1-\frac{\omega(p)}{p}\right)$$ （由(10.40)式）代入（10.56)式即得

$$G(z)\geqslant\frac{G_d(z/d)}{\prod_{p\mid d}\left(1-\frac{\omega(p)}{p}\right)}\qquad(10.57)$$

再注意到恒有$|\mu(d)|\leqslant1$,由（10.47）、(10.57)式即得

$$|\lambda_d|\leqslant1$$

于是

$$R\leqslant\sum_{\substack{d_1\mid P(z)\\ d_2\mid P(z)\\ d_1<z,\,d_2<z}}|r_{[d_1,d_2]}|\quad(\text{因 } d\geqslant z \text{ 时}\lambda_d=0)\qquad(10.58)$$

这样，我们就证明了下面的重要定理，此即最简单的塞尔伯格的上界筛法：

定理10.1 设对有限序列$\mathscr{A}$有条件(10.30)成立，则对任何$z\geqslant2$有

$$S(\mathscr{A};\mathscr{T},z)\leqslant\frac{X}{G(z)}+\sum_{\substack{d_1\mid P(z)\\ d_2\mid P(z)\\ d_1<z,\,d_2<z}}|r_{[d_1,d_2]}|$$

下面要给出定理10.1的一个简单应用，为此我们叙述一个引理，它的证明不能在这里给出。

引理10.9 设k_0为正整数，定义

$$H_{k_0}(x)=\sum_{\substack{d<x\\ (d,k_0)=1}}\frac{\mu^2(d)}{\varphi(d)}$$

则

$$H_{k_0}(x)\geqslant\prod_{p\mid k_0}\left(1-\frac{1}{p}\right)\ln x$$

现在考虑例10.1 中的序列$\mathscr{A}$，但改取 $y=x$。又取$\mathscr{T}=\{p:p\mid k\}$，于是$S(\mathscr{A};\mathscr{T},z)$ $(z\leqslant x)$就表示1，2，…，$[x]$这$[x]$个正整数中不能被 k 的小于z 的所有素因数整除的数的个数，如果定义

$$\Phi_k(x)=\sum_{\substack{n\leqslant x\\(n,k)=1}}1$$

那么显然得到

$$\Phi_k(x)\leqslant S(\mathscr{A};\mathscr{T},z)\qquad(10.59)$$

由对例10.1的讨论知道应取 $X=x$，$\omega(d)=1$ (若$\mu(d)\neq0,d\mid P(z)$)以及$|r_d|\leqslant1$。由(10.27)式就有

$$g(d)=\frac{1}{d\prod_{p\mid d}\left(1-\frac{1}{p}\right)}=\frac{1}{\varphi(d)}$$

$$\mu(d)\neq0,\ d\mid P(z).$$

这里用到（10.9）式.

由（10.28）式就有

$$G(z)=\sum_{\substack{d<z\\d\mid P(z)}}\frac{\mu^2(d)}{\varphi(d)}\qquad(10.60)$$

定义

$$k_0=\prod_{\substack{p<z\\p\in\mathscr{T}}}p$$

则易见

$$G(z)=\sum_{\substack{d<z\\(d,k_0)=1}}\frac{\mu^2(d)}{\varphi(d)}$$

$$\geqslant(\ln z)\prod_{p\mid k_0}\left(1-\frac{1}{p}\right)$$

$$=(\ln z)\prod_{\substack{p<z\\p\in\mathfrak{P}}}\left(1-\frac{1}{p}\right)\qquad(10.61)$$

这里用到引理10.9．又对余项有

$$\sum_{\substack{d_1\mid P(z)\\d_2\mid P(z)\\d_1<z,\,d_2<z}}\left|r_{[d_1;d_2]}\right|\leqslant\sum_{d_1<z}\sum_{d_2<z}1\leqslant z^2$$

(10.62)

将（10.61）、（10.62）式代入定理10.1并利用（10.59）式即得

$$\Phi_k(x)\leqslant\frac{x}{(\ln z)\prod\limits_{\substack{p<z\\p\in\mathfrak{P}}}\left(1-\frac{1}{p}\right)}+z^2$$

$$=\frac{x}{(\ln z)\prod\limits_{\substack{p<z\\p\nmid k}}\left(1-\frac{1}{p}\right)}+z^2,\ 对z\leqslant x$$

(10.63)

如果要求k的最大素因数（简记为$p(k)$）不超过x，那么就有

$$\Phi_k(x)\leqslant\frac{x}{\ln z}\cdot\frac{k\prod\limits_{p\mid k}\left(1-\frac{1}{p}\right)}{k}\cdot\frac{1}{\prod\limits_{p\mid k}\left(1-\frac{1}{p}\right)\prod\limits_{\substack{p<x\\p\nmid k}}\left(1-\frac{1}{p}\right)}$$

$$+z^2$$

$$=\frac{x}{\ln z}\ \frac{\varphi(k)}{k}\ \frac{1}{\prod\limits_{p<x}\left(1-\frac{1}{p}\right)}+z^2$$

从而

$$\frac{k}{\varphi(k)}\frac{\Phi_k(x)}{x}$$

$$=\frac{1}{\prod\limits_{p<x}\left(1-\frac{1}{p}\right)}\cdot\left(\frac{1}{\ln z}+\right.$$

$$\left.\frac{z^2k}{x\varphi(k)}\prod_{p<x}\left(1-\frac{1}{p}\right)\right)$$

$$\leqslant\frac{1}{\prod\limits_{p<x}\left(1-\frac{1}{p}\right)}\left(\frac{1}{\ln z}+\frac{z^2}{x}\right.$$

$$\left.\cdot\frac{k\prod\limits_{p<x}\left(1-\frac{1}{p}\right)}{k\prod\limits_{p\mid k}\left(1-\frac{1}{p}\right)}\right)$$

$$\leqslant\frac{1}{\prod\limits_{p<x}\left(1-\frac{1}{p}\right)}\left(\frac{1}{\ln z}+\frac{z^2}{x}\right)\quad(10.64)$$

我们已知，当 $x\geqslant286$ 时有以下不等式成立：

$$\prod_{p<x}\left(1-\frac{1}{p}\right)^{-1}\leqslant e^{\gamma}(\ln x)\left(1+\frac{1}{2\ln^2x}\right),$$

$$\gamma\approx0.5771\cdots\quad(10.65)$$

（证明这里不能给出），γ 称为尤拉常数。

再选取 $z=x^{1/3}$ 就由（10.64）、（10.65）式得到，当 $x\geqslant 286$ 时

$$\frac{k}{\varphi(k)}\frac{\Phi_k(x)}{x}\leqslant e^{\gamma}(\ln x)\left(1+\frac{1}{2\ln^2 x}\right)\left(\frac{3}{\ln x}+\frac{1}{x^{1/3}}\right) \qquad (10.66)$$

可以证明，（10.66）式右边的表达式是 x 的单调减少函数，于是当 $x\geqslant 286$ 而且 $x\geqslant e^6$ 时有

$$\frac{k}{\varphi(k)}\frac{\Phi_k(x)}{x}\leqslant e^{0.58}(\ln e^6)\left(1+\frac{1}{2(\ln e^6)^2}\right)\left(\frac{3}{\ln e^6}+\frac{1}{e^2}\right)$$

$$<(1.79)(6)\left(1+\frac{1}{72}\right)\left(\frac{1}{2}+\frac{1}{(2.7)^2}\right)$$

$$<7$$

于是，注意到 $e^6>286$，我们就最后得到以下的

定理10.2 若 $x\geqslant e^6$ 且 $p(k)\leqslant x$，我们就有

$$\Phi_k(x)<7\frac{\varphi(k)}{k}x$$

如果我们改取 $\mathscr{A}$ 为例10.2中的序列，而且令例10.2中的 x 为一个充分大的偶数。这时就对应要用到定理10.1中 $\omega(p)=p/(p-1)$（对 $p\nmid x$）的特例，对于定理10.1中的主项和余项经过较为复杂的估计可以推出有如下的结论成立：

定理10.3 设 x 为充分大的偶数，则不超

x 的素数 p 中，使 $p+2$ 也为素数的那种孪生素数对的对数不超过以下数值

$$8\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\frac{x}{\ln^2 x}\left(1+M\frac{\ln\ln x}{\ln x}\right)$$

这里 M 是一个与 x 无关的正常数。

完全类似地可以用定理10.1来研究序列

$$\mathscr{A}=\{x-p:p\leqslant x\}$$

这里 x 仍表示充分大的偶数，与定理10.3完全类似地可以证明

定理10.4 设 x 为充分大的偶数，则 x 可以表为两个素数之和的表示方法个数（注意 $x=p_1+p_2$ 与 $x=p_2+p_1$ 看成是两种不同的表示方法，这里 $p_1\neq p_2$）至多为

$$8\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{\substack{p>2\\ p\mid x}}\frac{p-1}{p-2}\cdot\frac{x}{\ln^2 x}\left(1+N\frac{\ln\ln x}{\ln x}\right)$$

这里 N 是一个与 x 无关的常数。

上两个定理就对孪生素数对个数及哥德巴赫偶数猜想的上界问题给出了相当好的回答。这两个定理的证明需要数论中更多更深入的知识，这里不能给出详细证明。

筛法在数论中有许多应用，这里不能详加介绍，有兴趣的读者可以去看英国数学家哈伯

斯坦(H.Halberstam)与西德数学家李希特(H.-E. Richert) 合著的《筛法》一书(《Sieve Methods》). 也可以看我国数学家潘承洞、潘承彪所著《哥德巴赫猜想》一书的第七章、第九章等内容。

附 录

我们用两种方法给出 λ_d 的导出方法。

方法一 引理10.5中等号成立之充要条件是有常数 c 使对一切 $n\leqslant m$ 有

$$\frac{a_n}{b_n}=c$$

于是使（10.48）式最后不等式中等式成立之充要条件为有常数 c 使对一切 $d<z$，$d|P(z)$ 有

$$\frac{\mu(d)\sqrt{g(d)}}{y_d/\sqrt{g(d)}}=c$$

即有 c 使 $$y_d=\frac{1}{c}\mu(d)g(d) \tag{10.67}$$

再由 $F=\sum\limits_{\substack{d<z\\d|P(z)}}\mu(d)y_d=1$，将(10.67)式代入此式即得

$$\frac{1}{c}\sum_{\substack{d>z\\d|P(z)}}\mu^2(d)g(d)=1$$

此即

$$c=\sum_{\substack{d<z\\d|P(z)}}\mu^2(d)g(d)=G(z)$$

于是应取

$$y_d=\frac{1}{G(z)}\mu(d)g(d) \tag{10.68}$$

由（10.44）式并用莫比乌斯反转公式即得

$$\lambda_d\frac{\omega(d)}{d}=\sum_{\substack{l|P(z)\\d|l,\,l<z}}\mu\left(\frac{l}{d}\right)y_l \tag{10.69}$$

将（10.68）代入（10.69）式即得

$$\lambda_d \frac{\omega(d)}{d}=\frac{1}{G(z)}\sum_{\substack{l|P(z)\\ d|l\\ l<z}} u\left(\frac{l}{d}\right)\mu(l)g(l)$$

$$=\frac{1}{G(z)}\sum_{\substack{dk|P(z)\\ (k,d)=1,\, dk<z}} \mu(k)\mu(dk)g(dk)\quad (\text{令 } l=dk)$$

$$=\frac{\mu(d)g(d)}{G(z)}\sum_{\substack{k|P(z)\\ (k,d)=1\\ k<z/d}} \mu^2(k)g(k)$$

$$=\frac{\mu(d)g(d)}{G(z)}G_d\ (z/d)$$

此即所欲证者。

方法二　此即在 $F=1$ 之限制条件下求 T 之极值问题，我们应用拉格朗日不定乘数法，作拉格朗日函数

$$L=T+\eta F \qquad (\eta\text{为待定常数})$$

由

$$\frac{\partial L}{\partial y_r}=0,\ r=1,\ 2,\ \cdots,\ [z],\ r|P(z)$$

容易解出

$$y_r=-\frac{\eta}{2}\mu(r)g(r),\ r=1,\ 2,\ \cdots,[z],r|P(z) \tag{10.70}$$

代入 $F=1$ 中与证法一同样可解得

$$\eta=-2\Big(\sum_{\substack{d<z\\ d|P(z)}}\mu^2(d)g(d)\Big)^{-1}=\frac{-2}{G(z)}$$

将 η 值代入（10.70）式即得

$$y_r=\frac{\mu(r)g(r)}{G(z)},\ r=1,\ 2,\ \cdots,\ [z],\ r|P(z)$$

这又得到（10.68）式，下面证明与上同，不再赘述。